التعاون الأوروبي القضائي والأمني
كنموذج لمكافحة الجرائم الحديثة

د. جنان الخوري الفخري(*)

يعدّ الاتحاد الأوروبي مختبرا إقليميا Un laboratoire régional لتطوّر القواعد الجديدة للقانون الجزائي الدولي. في الواقع، ان الاتحاد الأوروبي، وبصفته إقليماً متكاملاً لا سيما بعد **اتفاقية شينغين** *Schengen* التي فتحت حدود ثلاث عشرة دولة على بعضها، وأزالت نقاط التفتيش عن الحدود الداخلية، فأصبح سريع التأثّر بشكلٍ خاص بإشكاليات الإجرام المنظم العابر للحدود(١). ففي الواقع، لم تفد حرية تنقّل الأشخاص وحرية تداول الأشخاص العاديين والمجرمين، الذين ينظمون أنفسهم بطريقة يزيدون فرص تحقيق فوائدهم، من جهة، وتقليل مخاطر الملاحقة والمحاكمة، من جهةٍ أُخرى(٢).

الأمر الذي دفع المجلس الأوروبي إلى التنبّه إلى هذه الظاهرة فعمد إلى المبادرة لمكافحتها، وبدأ يصدر تقريرا سنويا عن تطوّر الجريمة المنظمة(٣) ويتبنّى كثيراً من المشاريع الهادفة إلى حماية المجتمع الأوروبي عبر مراقبة الجريمة المنظمة، تحسين التحقيق والتنسيق، تبادل التقنيات وضرورة تقارب التشريعات العقابية الأوروبية من بعضها البعض(٤)... بهدف فاعلية التحقيق العام للحدود والتقنيات المستخدمة، ضرورة مكافحة تبييض الأموال وحماية العاملين في الجهاز القانوني المختص.

(*) أستاذة القانون الجزائي في الجامعة اللبنانية.

(١) Convention dapplication de lAccord de Schengen du 14 juin 1985 relatif à la suppression graduelle des contrôles aux frontières communes, 19 juin 1990, Schengen, www.europa.eu

(٢) Christine Van De Wyngaert: Rapport général: Les transformations du droit international pénal en réponse de la criminalité organisée - XVIIe congrès international de droit pénal - Rapport général - Colloque préparatoire - R.I.D.P. - 1996, p48.

(٣) Europol: Rapport 2003 sur la criminalité organisée dans lUnion Européenne, Version publique, La Haye, le 21 oct. 2003, p5.
http://www.europol.europa.eu/publications/EUOrganisedCrimeSitRep/2003/OCSitRep2003_fr.pdf

(٤) Conseil de justice et des affaires intérieures (JAI): Le programme daction, prévention et contrôle de la criminalité organisée: une stratégie pour le prochain millénaire, J.O.C.E - 3 mai 2000, C. 124, p1.

كما أن بعض المواد في معاهدة أمستردام لعام ١٩٩٧ تعكس الاهتمام المتنامي للإجرام المنظم. بحيث تضيف المادة ٢٩ منها الى لائحة أهداف الاتحاد، التعاون الوثيق بين السلطات القضائية، الشرطة، السلطات الجمركية وباقي السلطات المختصة في الدول الأعضاء.

توسع المادة ٣٠ (ف. ٢) من هذه المعاهدة المهام الموكلة الى اليوروبول وتتبنّى المادة ٣١ الاعتماد المتطور للتدابير المنشئة للقواعد الدنيا المتعلقة بالعناصر المكونة للجرائم الجزائية وللعقوبات المطبّقة على الإجرام المنظّم، الإرهاب والاتجار بالمخدرات.

كما وضع المجلس الأوروبي أولويات العدالة والقضايا الداخلية لفترة ما بين تموز ١٩٩٦ وحزيران ١٩٩٨ حيث أتت الجريمة المنظمة والاتجار بالمخدرات في المرتبة الثانية بعد الإرهاب(٥).

أما إحدى التحولات الهامة في مسائل التعاون الشرطي في أوروبا خلال السنوات الأخيرة، فتكمن في عديد من المعاهدات المختصة. وبعد نجاح هذا الاتحاد في إقامة دعائم بنيانه الاقتصادي، السياسي والمالي، أصبح يرنو إلى بناء قضاء أوروبي موحد لمكافحة الجرائم التي تهدد النظام العام الأوروبي. حيث تجسّد اليوم في مؤسستين بالغتَي الأهمية تشكلان الخطوة الأولى في هذا الصدد، وهما الشبكة القضائية الأوروبية أو مكتب الشرطة الأوروبية EUROPOL(٦) ١٩٩٥ وجهاز العدالة الأوروبية EUROJUST ٢٠٠٢؛ بالاضافة الى **اتفاقية** Schengen ١٩٩٠ واتفاقية متعلقة بالتعاون الجمركي لعام ١٩٩٧. حيث تنظم هذه الاتفاقيات التعاون القضائي والشرطي بشكلٍ تفصيليّ وهذا ما سنبينه في فرعيين متتاليين.

الفرع الأول
مكتب الشرطة الأوروبية:

يهدف هذا المكتب الى تعزيز التعاون بين السلطات المختصة لمكافحة كل أشكال الجريمة المنظمة لا سيما الاتجار بالمخدرات. تتمثّل مهمته الأساسية على الصعيد الأوروبي في تسهيل تبادل المعلومات بين الدول الأعضاء، جمع المعلومات، تحليلها وتعميمها، التعاون وتيسير التحقيقات، إدارة قواعد البيانات ذات الصلة، تطوير الخبرة الفنية في الميادين الأساسية للجريمة(٧).

كما انه يختص بالتحديد في الجريمة المنظمة، الاتجار بالمخدرات، الاتجار بالرقيق الأبيض، تهريب المهاجرين، تزوير العملات، أيضاً الاتجار بالسيارات المسروقة والإرهاب والاتجار غير المشروع بالمواد الشعاعية والنووية...

أما على الصعيد الدولي – وكما ذكرنا – فتتمثّل مهمته في التعاون مع الأنتربول الدولي

(٥) Résolution du conseil du 14 oct 1996, Fixation des priorités de la coopération dans le domaine de justice et des affaires intérieures (JAI) pour la période du 1er juillet 1996 au juin 1998, J.O.C.E, 20/10/1996, C. 319, p1.

(٦) Convention portant création dun office européen de police (convention Europol), 26 juillet 1995, Bruxelles, J.O.C.E., 27 novembre 1995, C. 316, p33.

(٧) م. ٢ من اتفاقية يوروبول المستندة الى K.3 من معاهدة الاتحاد الأوروبي في خصوص إقامة مكتب أوروبي للشرطة، وهي شبكة مشكلة من قضاة الدول الأعضاء في الاتحاد الأوروبي، يشكلون نقاط اتصال هذه الشبكة، تتمثل مهمتهم الأساسية في توفير المعلومات العامة (التشريع القابل للتطبيق، التنظيم القضائي) والمعلومات الخاصة (التعريف بالقضاة المكلفين في بلدانهم ملفات خاصة) أو توفير الدعم الفني الصرف/http://www.europol.eu.int .

لوضع الاستراتيجيات والوسائل المشتركة للتصدّي للإجرام من خلال التعاون، التنسيق، التمثيل المتبادل، تبادل المعلومات الميدانية والفنية وتنسيق الأنشطة، بما في ذلك تطوير المعايير المشتركة، خطط العمل، التدريب، الأبحاث العلمية وإعارة ضباط الارتباط (المواد ٣-٤-٥ من اتفاق التعاون).

من جهةٍ أخرى، يتصدّر **الاتجار بالبشر** أولوية التعاون بين الأنتربول واليوروبول ويتمحور التعاون حول أنواع الإجرام الدولي الحديثة لا سيما:

- وثائق السفر المسروقة.
- الاتجار في البشر.
- خلاعيات الأطفال المتداولة عبر الانترنت.
- الإجرام المرتبط بتكنولوجيا المعلومات.
- الإجرام المنظّم محليا وعالمياً ومدى التغيير المستمر والنشط للمجرمين.
- حسن التبادل الفوري والمأمون للمعلومات الشرطية الحيوية.
- كيفية تعزيز التعاون الشرطي في الجرائم ذات الأبعاد العالمية.
- سعي المكاتب المركزية الوطنية إلى التبادل الفاعل للمعلومات والتقارير بشأن المسائل الإجرامية.
- التخطيط لعمليات الأمن الكبرى في الإقليم الأوروبي(٨).

بالفعل، أثمر التعاون بين المنظمتين عملية دولية ضد الاستغلال الجنسي للأطفال بمشاركة السلطات الإيطالية وستين دولة أخرى في أوروبا، أميركا، آسيا وأفريقيا، فضلا عن اوستراليا: أطلق عليها اسم "القناة الكبيرة"(٩).

هناك " "l'Opération Maxim، عام ٢٠٠٤ وبفضل تنظيم جيّد لمهمة اشترك فيها أربعة بلدان أوروبية، تمّ توقيف ٨ أشخاص في المملكة المتحدة، بتهمة الاشتراك في التعاون للاتجار بالأشخاص، ثم تبعتها عدّة توقيفات مشابهة في دول أوروبية(١٠).

أما عن دور الـ يوروبول في مكافحة الانترنت، فأعرب رئيس الـ يوروبول أدولف هيغل عن خلاصة رأيه أمام مؤتمر (كوميسيك) لأمن الكومبيوتر سنة ٢٠٠٢ كما يلي:

"بالنسبة الى جرائم الانترنت، يبدو أننا خسرنا المعركة قبل أن نبدأ القتال.. إذ لا نستطيع مجاراتها."

هكذا، وضعت جرائم الإنترنت الواسعة النطاق أجهزة الشرطة في جميع أنحاء العالم أمام حيرة كيفية مواجهتها؛ ولقيام اليوروبول بواجباته تم تأسيس "**مركز جرائم التكنولوجيا المتقدمة**" كأحد الفروع التابعة لليوروبول الذي يؤمل منه أن ينجز تنسيقاً فاعلاً وحاسماً في الحد من الجرائم المقترفة، بواسطة الإنترنت عبر الحدود المفروضة بين بلدان أوروبا.

ختاماً، هذه كانت أهم مهام "اليوروبول" وأنشطته، أمّا بالنسبة الى الأوروجست أشكال

---

(٨) مؤتمر الانتربول الإقليمي- الأوروبي السنوي من ٢٥ إلى ٢٧ أيار/مايو ٢٠٠٥ (نقوسيا-قبرص):
http://www.interpol.int/Public/ICPO/PressReleases/PR2005/PR200518Ar.pdf

(٩) عملية واسعة النطاق شارك فيها زهاء ٤٠٠ شرطي في العملية فقاموا بعمليات دهم في جميع المناطق الإيطالية والقوا القبض على أربعة أشخاص. تقدم هذه العملية دليلا جديدا على فاعلية" الشرطة لمكافحة هذه الجرائم - ٢٠٠٤/١١/٢٦
http://www.bab.com/news/full_news_print.cfm?id=63323

(١٠) "Spécial Cooperation on human Trafficking، ٢٠٠٤/١١/٤.
http://www.homeoffice.gov.uk/eupresidency2005/organised_crime.html#human_trafficking

التعاون الأخرى على الصعيد الأوروبي، فالإجابة في الفرع الأخير من هذا البحث.

الفرع الثاني
جهاز العدالة الأوروبية

يتالف "جهاز العدالة الأوروبية" أو الأوروجست[١١] من ٢٥ قاضياً (لكل دولة عضو واحد)؛ تتمثل مهمتهم الأساسية في ضمان تبادل المعلومات القضائية العملياتية، تأمين التنسيق في ممارسة العمل العام داخل الدول المعنية، لا سيما في مجال تنفيذ طلبات التعاون القضائي في كثير من الدول الأعضاء، بهدف تنشيط التحقيقات والملاحقات القضائية وتنسيقها، تنفيذ طلبات تسليم المجرمين، دعم السلطات المختصّة بغية جعل تحقيقاتها وملاحظاتها القضائية أكثر فاعلية[١٢].

على رغم من أنّ لكل منهما اختصاصه، نظامه وتركيبته، يتكامل كل من Europol و Eurojust ويتعاونان في مكافحة هذه الجرائم[١٣]يركزان جهودهما على عدد محدود من القطاعات ذات الأولوية ومنها الجرائم المالية، تبييض الأموال، الفساد، تزييف عملة اليورو، الاتجار بالأفراد، سوء استغلال الأطفال جنسيا، جرائم التكنولوجيا وجرائم البيئة...

أما التغييرات التي طرأت على القانون الإجرائي فهي أكثر وضوحاً، في ما يختص بالمفاهيم التقليدية للشرطة والتحقيقات الجنائية، بحيث نلاحظ تغييراً جذرياً في طرق تصرّف الشرطة، منتقلين من شرطة réactive للتوجّه نحو شرطة Proactive[١٤] فالتقنيات الحديثة التي كانت مخصصة فقط لأجهزة الأمن، أصبحت اليوم في خدمة الشرطة (كالتنصت الهاتفي، جمع المعلومات وتشكيل ما يسمى بنك المعلومات).

تقود الجريمة المنظمة، على الصعيد الوطني، الى إجراء عدة تغييرات: كتقنيات التحقيق الحديثة والمتطورة، تسجيل الأحاديث، حفظ الصور، ومراقبة تحرك الأشخاص أو البضائع... من خلال أساليب متعددة:

التسليم المراقب وإشتراك الشرطة في بعض العمليات من خلال التخفّي وغيرها بما يعرف بالـ Pro activation... حيث لم يعد هدف العديد من التحقيقات والملاحقات وجمع المعلومات والأدلة، معاقبة الجريمة، إنما أيضاً الحيلولة دون وقوعها ومصادرات أموال المنظمات الإجرامية[١٥].

كما أن هناك وسائل حديثة للإتصال، كالسلطات المركزية، **مكاتب ارتباط**، بهدف تحسين تبادل المعلومات بين سلطات الشرطة والتعاون الشرطي الدولي.

تنص على تبني هذه التقنيات العديد من الإتفاقيات كإتفاقية الإتحاد الأوروبي لعام ١٩٩٠ لمكافحة تبييض الأموال (م٢٣,) وإتفاقية Schengen (م٣٩,–٨٣) التي تنص على نظام

(١١) Conseil de l'Europe: Décision instituant Eurojust afin de renforcer la lutte contre les graves de criminalité - 28 fév.2002 - 2002/187/JAI - Bruxelles - J.O. C.E. - L. 63 - 6 mars 2002 - P: 1 - entrée en vigueur le 6 mars 2003.

(١٢) Nadine Thwaites: Eurojust autre brique dans l'édifice de la coopération judiciaire en matière pénale ou solide mortier - Rev.sc.crim., 2003, p50.

(١٣) Serge Brammertz, Pierre Berthelet: Eurojust et le réseau judiciaire européen: concurrence ou complémentaire, R.D.P.C., 2002, p389 et suiv.

(١٤) Les transformations du droit international pénal en réponse au défi la criminalité organisée, op.cit., p42

(١٥) Van Den Wyngaert: Rapport general, op. cit., p612.

معلوماتي مختص بهدف تبادل طلبات المساعدة (Le système informatique Schengen SIS) والتي تنص على دعوة الدول الأطراف الى عقد إتفاقيات ثنائية بهدف تسريع عمليات التعاون (م٤٧,). نجد النص ذاته في اتفاقية اليوروبول Europol (م٥,) والمادة ٣٢ من معاهدة أمستردام.....

وفي السياق ذاته، يشكل **فريق التحقيق المشترك** نوعاً آخر من التبادل الهام للمعلومات، هذا ما شجعت عليه اتفاقيات كثيرة (اتفاقية فيينا لعام ١٩٨٨) اتفاقية الاتحاد الأوروبي المتعلقة بالتعاون الجمركي لعام ١٩٩٧[١٦] التي انعقدت بين بعض الدول الأوروبية فقط.

بدورها، أجازت اتفاقية شينغين السماح لموظفيّ إنفاذ القوانين التابعين لإحدى الدول، بإجراء عمليات مراقبة محدودة في دولة أخرى، كما تضمّنت إمكانية محدودة في المطاردة الساخنة للفارين من العدالة العابرين للحدود إلى إقليم دولة أخرى، والتسليم المراقب كمراقبة النشاط غير المشروع، مثل عملية الاتجار بالمخدرات من بدايتها إلى نهايتها.

كما يتضمّن نظام شينغين للمعلومات (SIS) إدخال البيانات في شأن الاشخاص الذين جرى إبعادهم من البلد، أو الذين يوجد في شأنهم أمر صريح بالقبض عليهم، وتستطيع السلطات المماثلة في كل دولة مشاركة في اتفاقية شينغين ان تدخل البيانات بشكلٍ مباشر في النظام.

وهنا يمكن القول، إن إنشاء أجهزة مماثلة لليوروبول والأوروجست، في العالم العربي **قد يكون أمرا مفيدا في مكافحة الجريمة المنظمة والاقتصادية، وفي وضع آليات عمل تنفيذية لكثير من الاتفاقيات الدولية المناهضة للإرهاب والجريمة المنظمة.**

على **الصعيد العربي**، اتخذت خطوات خجولة من خلال إنشاء "مجلس وزراء الداخلية العرب لـ "شعبة اتصال عربية"، مهمتها ملاحقة الجريمة المنظمة عبر الحدود. أما الخطوة الهامة، فتتبدّى من خلال **التعاون بين الأنتربول ووزراء الداخلية العرب** لتبادل البيانات الشرطية وحثّ خطى التعاون الفني بين المجموعة الشرطية العربية والأنتربول، أيضاً توسيع عرى التعاون الشرطي الدولي في مكافحة الإجرام المنظم وتوثيقها[١٧].

كما يعمل **البرنامج الدولي للمساعدة والتدريب على التحقيق الجزائي** (ICITAP) على الترادف مع مكتب المساعدة والتدريب على تعزيز القدرات التحقيقية لدى أجهزة الشرطة في البلدان النامية[١٨].

كما تطرقت **الحلقة الدراسية الأولى للشراكة الأورو-متوسطية** Euro Med لمكافحة الجريمة الإلكترونية إلى الشق البوليسي لحماية البنى التحتية للمعلومات المهمة، التدريب، جمع الأدلة وتحليلها وإنشاء وحدات متخصصة وإدارتها لمكافحة الجريمة الإلكترونية[١٩].

---

(١٦) Convention relative à l'assistance mutuelle et à la coopération entre les administrations douanières - 18 décembre 1997, Bruxelles, J.O.C.E., 23 janv.1998, C. 24, p1.

(١٧) www.arabeleagueonline.com

(١٨) International Criminal Investigative Training and Assistance Programm (ICITAP) www.usdoj.gov/criminalicitap.html

(١٩) الحلقة الدراسية التدريبية الأورو-متوسطية الأولى حول الجريمة المعلوماتية، ١/ ٥ تشرين الثاني ٢٠٠٥، بريطانيا. http://www.eu-delegation.org.eg/AR/docs/news18.asp

حديثاً، أطلقت **الحكومة البريطانية «وكالة الجريمة المنظمة الخطيرة»** (سوكا) باعتبارها النسخة البريطانية من مكتب المباحث الفيديرالي (اف. بي. آي) الأميركي، تضم ٤ آلاف ضابط، ومنحتها صلاحيات واسعة لمواجهة كل أوجه الجرائم المنظمة(٢٠).

نستنتج ممّا تقدّم، أن النموذج التقليدي، الذي يقضي بألا تتعامل السلطات القضائية مع بعضها بعضا بشكل مباشر، إنما بواسطة الطرق الديبلوماسية، أصبح في عداد القواعد القديمة في قريةٍ كونية تتحول يوماً بعد يوم إلى مجتمع إلكتروني، لا سيما في ما يختص بتعقّب المنظمات الإجرامية التي تستفيد من التطورات التكنولوجية الحديثة؛ لذلك تميل المعاهدات الحديثة إلى التعاون الدولي وتنظم الاتصال المباشر بين السلطات القضائية.

ختاما، يجب على الشرطة التي اتخذت صفة Proactive، في تطبيقها قواعد قانون العقوبات الدولي احترام مبدأ الشرعيةPrincipe de légalité ، مبدأ التناسب Principe de Proportionnalité ومبدأ "المتهم بريء حتى إثبات إدانته"...

الفرع الثالث
التعاون الأوروبي لحماية البيانات ذات الطابع الشخصي

في الواقع، وبقدر ما يعتمد الإنسان على التكنولوجيات الحديثة في العصر الراهن، كضرورة من ضرورات الحياة، لا سيما لناحية المعرفة والثروة وحرية التعبير، بقدر ما تصبح حياته الخاصة، أكثر عرضة للتهديدات والاعتداءات و"التطفّل"، والاستثمار، والاستغلال، وتعديل بياناته الشخصية(٢١)... وفي الواقع، تُثير مسألة حقوق الإنسان بشكل عام، والخصوصية وحماية المعطيات ذات الطابع الشخصي بشكل خاص – سواء بوجهها التقليدي أم الإلكتروني الحديث(٢٢) – كثيراً من الإشكاليات، وأبرز التحديات المادية والمعنوية والتقنية، التي ستواجه العالم، بشكل عام، والدول العربية بشكل خاص، حيث لا تزال تحتل كل من الحياة الخاصة، والعائلة مكانة أساسية في العلاقات الاجتماعية، في وقت باتت معظم بيانات الأفراد، متاحة بأشكال مختلفة، على المواقع الإلكترونية. ما آثار، انشغال هذه الدول– ومن بينها المملكة المغربية – لإيجاد أطر قانونية حديثة، لصون خصوصية المعطيات، وحماية هوية الأفراد الإلكتروني Electronic idendity في العالم الرقمي، عبر مراجعة القوانين والتنظيمات المرعية الإجراء، المتعلقة بحماية المعطيات ذات الطابع الشخصي، والحق في الخصوصية، أو في سن تشريعات حديثة، لسد الفراغ التشريعي، ولمواجهة تحديات تطورات التكنولوجيا الرقمية، ولإيجاد وعاء تطبيقي لهذه المعطيات، والتي لم تعد لها قيمة مادية ملموسة فحسب، بل غدت أرقاما وعلامات ومعايير؛ تترافق مع حفظ هذه المعطيات، وتخزينها، واسترجاعها، وتحليلها، ومعالجتها، ونقلها، عبر شبكة.الإنترنت، دون أي اعتبار للحدود الجغرافية أو السيادية. في مقابل غياب،

(٢٠) جريدة الشرق الأوسط، الثلاثاء ٤/٤/٢٠٠٦، على موقعها الالكتروني التالي:
http://www.asharqalawsat.com/details.asp?section=4&issue=9989&article=356465

(٢١) EMOINE (Vincent): Le régime juridique des constatations policières sur internet, L"Harmattan, 2014, Paris, p93.

(٢٢) ROQUES-BONNET (Marie-Charlotte): la droit peut-il ignorer la révolution numérique, 2010, Michalon, p413.

أو ضعف البنية التحتية الرقمية، وغياب الإطار القانوني والتنظيمي، وعدم وجود البيئة الملائمة للفضاء السيبراني، ونقص الوعي أو ثقافة المعلوماتية.

على الصعيد العالمي، يعتبر "**الحق في الخصوصية**"، أحد الحقوق اللصيقة بشخصية الإنسان التي تتثبت له بمجرد كونه إنساناً، وأحد أوجه حقوقه الأساسية[٢٣]، المعترف به في المواثيق والصكوك الدولية، لا سيما الإعلان العالمي لحقوق الإنسان لعام ١٩٤٨[٢٤]، والعهد الدولي الخاص بالحقوق السياسية والمدنية، والاتفاقية الأوروبية لحماية حقوق الإنسان والحريات، والاتفاقية الأميركية لحقوق الانسان، والتي تؤكد على عدم جواز التدخل التعسفي، في حياة الأفراد، أو مراسلاتهم، وحقهم في حماية قانونية.

وفي المقابل، يبرز "**الحق في التعبير**"، بدوره كأحد الحقوق الإنسانية، المعترف بها عالميا وفي دساتير أغلبية الدول وقوانينها. وتطرح الإشكالية الأساسية، في اختلاف الأنظمة القانونية، ذات الفلسفة والثقافة المتخلفتين، ما ينعكس على تحديد الأولوية بين هذين الحقين: الحق في التعبير والحق في الخصوصية. وإذا ما راجعنا قواعد الاتحاد الأوروبي وإرشاد الإسكوا (المادة ٨)[٢٥] وبعض القوانين أو الأنظمة الفرنسية، فنراها تولي الأهمية للحق في الخصوصية، وبإشراف اللجنة الوطنية للمعلوماتية والحريات Commission Nationale de l'Informatique et des Libertés (CNIL)، بينما نرى العكس في الولايات المتحدة، حيث تكتسب البيانات الشخصية، قيمة تجارية، أكثر منها خصائص الميزات الشخصية[٢٦]. وبالطبع يغيب الحق في التعبير، في الدول ذات الأنظمة القمعية.

فماذا يثير مسألة تعريف **الحق في الخصوصية، وكيفية الاعتداء عليه، والصلة بين البيانات الشخصية او الحق في الخصوصية؟ والاطار القانوني لهذه الخصوصية؟**

لقد شكّلَ الإرشادُ الأوروبيّ لعام ١٩٩٥

(٢٣) هذا ما اكدت عليه اللجنة المعنية بالحقوق المدنية والسياسية في معرض تعليقها على المادة (١٧) من العهد والمتعلقة بالحق في حرمة الحياة الخاصة للفرد حيث أشارت إلى انه "يجب أن ينظم القانون عمليات جمع وحفظ المعلومات الشخصية باستخدام الحاسوب وغيرها من الوسائل، سواء أكانت تجريها السلطات العامة أم الأفراد العاديون أو الهيئات الخاصة. ويتعين إن تتخذ الدول تدابير فعالة لكفالة عدم وقوع المعلومات المتعلقة بالحياة الخاصة للشخص في أيدي الأشخاص الذين لا يجيز لهم القانون الحصول عليها، وعدم استخدامها على الإطلاق في أغراض تتنافى مع العهد. ولكي يتسنى حماية الحياة الخاصة للفرد على أكفأ وجه ينبغي أن يكون من حق كل فرد أن يتحقق بسهولة من ماهية البيانات المخزنة، والغرض من الاحتفاظ بها، كما ينبغي أن يكون بمقدور كل فرد أن يتحقق من هوية السلطات العامة أو الأفراد العاديين أو الهيئات الخاصة التي تتحكم في هذه البيانات، وإذا كانت هناك بيانات شخصية غير صحيحة أو بيانات جمعت أو جهزت بطريقة تتعارض مع أحكام القانون، ينبغي أن يكون من حق كل فرد أن يطلب تصحيحها أو حذفها".

(٢٤) بحيث تنص المادة ١٢ منه على "حق الشخص بعدم التعرض الإعتباطي لخصوصيته، وحقه في حفظ كرامته وحقوقه الفردية".

(٢٥) الارشاد الرابع - معالجة وحماية البيانات ذات الطابع الشخصي . المادة ٨: معالجة البيانات ذات الطابع الشخصي وحرية التعبير: "تعتمد الدول المتعاقدة بالنسبة لمعالجات البيانات ذات الطابع الشخصي، المنفذة لغايات الصحافة أو التعبير الأدبي أو الفني، اعفاءات من التقيد بأحكام هذا الإرشاد شرط احترام الحياة الخاصة" . ارشادات الإسكوا للتشريعات السيبرانية . مشروع تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية . اللجنة الاقتصادية والاجتماعية لغربي آسيا . إدراة تكنولوجيا المعلومات . ٢٠١٢ - بيروت . ص: ١٠١

(٢٦) TURK (Alex): "Pour les américains, les données personnelles sont des données commerciales qui ont une valeur marchande. En Europe, nous pensons que ce sont des attributs de la personnalité". http://eulogos.blogactive.eu/200/11/23/1%2%80%99oubli-numerique-futur-droit-con

(EC/46/95) تاريخ ٢٤/١٠/١٩٩٥، والمُتعلّق بِحماية الأشخاصِ الطبيعيين إزاءَ معالجة البياناتِ ذات الطابعِ الشخصيّ والتداول الحُرّ بِها، النواةَ الأوروبيةَ الأولى الراميةَ إلى حمايةِ البياناتِ الشخصيةِ المتوافقةِ مع السياسةِ الأوروبيةِ الراميةِ إلى حماية حقوقِ الإنسانِ، وقد اقتصَرَ تطبيقُ هذا الإرشاد على نِطاق الاتحاد الأوروبيّ.

وتنص المادة ٢٥ من الإرشادِ على منع تبادُل البيانات مع دُول خارج الاتحادِ الأوروبيّ[٢٧] لا تؤمِّن حماية مُوازيَة للحمايَة التي تُؤمّنها الدُول الأوروبيّة[٢٨]. وتُعتبرُ "اللجنة الأوروبية" هي المرجَع الصالح لاعتبار ما إذا كانت الدولة الثانية تُؤمّن الحمايةَ ذاتها. ولغايَةِ تاريخِه، تُعدُّ الدولُ التي تؤمّن الحمايةَ عينها من خارج الاتحاد الأوروبي، قليلةَ العددِ، وهي كندا والأرجنتين وأوروغواي ونيوزيلاند وسويسرا وآندور وجرساي وجزر غيرنسي وجزيرة آيل أوف مان.

في السِياقِ عَيْنه، تمَّ عقدُ اتفاق الملاذ الآمن" Safe Harbor Agreement ("أو اتفاقُ المِيناء الآمن")[٢٩] مع الولاياتِ المُتحدةِ الأميركيةِ عام ٢٠٠٠[٣٠]، والذي يُلزمُ الشركاتِ الأميركيةَ بعديد من المبادِئ التي تمنعُ الاعتداءَ على البياناتِ الشخصيةِ، وأبرزها: مُوجِبُ الإعلام وتَحديدُ الغاية من جمع المعلومات واستخدامها أو نقلِها للغير؛ حقُّ قُبول نقل المعلوماتِ للغير، أو الرفض والتزام الغير بمبادئ الملاذِ الآمنِ؛ حقّ الوصول إلى المعلوماتِ المُستقاةِ وتصحيحِها، إضافَةً إلى أمنِ المعلوماتِ ، وصحَّة البياناتِ، وإيجاد آلياتِ للاعتراض والتطبيقِ والنظرِ في شَكاوى المُتضرّرين وتقرير العُطْلِ والضرَرِ.

ولا بُدّ من ذِكر "اتفاق الولايات المتحدة الأميركيّة مع الاتحادِ الأوروبيّ"، اتفاق واشنطن لعام ٢٠٠٤[٣١]، الذي يفرضُ على الاتحادِ التأكُّد من التزام الناقليين الجويين بِتقديم كل المعلوماتِ المَطلوبَةِ لسلامَة الطيرانِ. حيث ألزمَ هذا الاتفاقُ أميركا بِضماناتٍ لتأمين الحمايةِ عينها المحدّدة من قبل الاتحادِ الأُوروبيّ. وفي عام ٢٠١٢، وقّع الفريقان اتفاقاً آخر Safe Harbor (الملاذ الآمن او الرصيف الآمن)[٣٢]، يتضمّنُ نقلَ بياناتِ المُسافرين وتحليلها، وحصر أهدافِه في مكافحة الإرهابِ، والاتجارِ بالمُخدراتِ، والاتجارِ بالرقيقِ، وسائِر الجناياتِ، والاحتفاظِ بهذه البيانات لمدّة عشر سنوات، ضِمن إطارِ تعاونٍ قانونيّ وتنظيميّ وأمنيّ. علماً بأن هذا الاتفاقَ لا يُقدّم الأمانَ إلا إلى الشركاتِ الكُبرى.

(٢٧) BENBOUSSAN: Traitement des opérateurs acheminant du trafic international, p798.

(٢٨) FERAL-SCHUL (Christiane): Cyberdroit, Le droit à l'épreuve de l'internet, 2009-2010, Dalloz, p83.

(٢٩) US-EU: International Safe Harbor Privacy Principles
https://en.wikipedia.org/wiki/Safe_Harbor_Principles#cite_note-inval-9

(٣٠) European Court of Justice 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.) 25 August 2000, retrieved 30 October 2015.

(٣١) Commission Européenne: Décision 2004/535/EC, JOUE, 225, 6 JUILLET 2004, p11-22.
http://eur-lex.europa.eu/LexUriSerc/site/en/oj/2004/l_235l_23520040706enoo110022.pdf

(٣٢) Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security - Official Journal L 0215, 11/08/2012 P. 5 - 0014

على الصعيدِ القضائيّ، وفي ٦ اكتوبر ٢٠١٥، قضَت المحكمةُ العُليا للاتحاد الأوروبيّ بِبُطلان "اتفاق الملاذ الآمن"[٣٣] لتبادل البياناتِ مع أميركا بعد قضيةِ "فيسبوك"، مُعتبرةً أنّه لا يمكن للشركةِ المذكورة أنْ تُسلّم بياناتِ المُستخدمين إلى السلطاتِ الأميركيةِ. وعلّلت المحكمةُ البُطلان بأنَّ شركةَ فيسبوك وعدداً من شركاتِ التكنولوجيا الأُخرى، وهي غوغل وأمازون، قد اسْتغلَّتْ هذا الاتفاقَ وأقدمَت على نقل بياناتِ المُستخدمين، وبِكمياتٍ ضخمةٍ، لأجهزتِها في الولاياتِ المتحدةِ الأميركيةِ، حيث سيتُمّ الاحتفاظُ بها هناك. وبالطبعِ، سينعكسُ هكذا الحكمُ على جميع الشركاتِ الأميركيةِ، التي تتعامَلُ مع بياناتٍ أوروبيَةٍ، بما في ذلك تويتر ومايكروسوفت وياهو وغوغل.

أما بالنسبةِ إلى المُستهلكين في منطقةِ الاتحادِ الأوروبيّ والمُتعاقدين مع مُزوّدي خدمات السحابة وغير الخاضعين "للملاذ الآمن"، فعليهم أنْ يخضعوا إلى تشريعاتِ الاتحادِ الأوروبيّ حول تصديرِ البياناتِ الشخصيةِ. وقد أنشأَتْ مؤسسة أمازون، على سبيل المِثال، موقعاً أوروبياً للحوسبَة السحابيةِ يُوفّرُ الثقةَ للمُستهلكين في أنَّ البياناتِ لن تُنقل عبر الحدودِ بالشكلِ الذي يُعدّ انتهاكاً للتوجيه الأوروبيّ. وهنا لا بدّ من ذكر التَوصية الأوروبية[٣٤] تاريخ ٢٤ اكتوبر ١٩٩٥ حول حِمايةِ الأشخاصِ فيما يتعلق بمعالجةِ البياناتِ ذات الطابعِ الشخصي، وحريّة نقلِ المُعطياتِ بما فيها البيانات الطبيّة والوِراثية.

عام ٢٠١٠، أصدرَت المفوضية الأوروبيةُ "نماذجَ بنودٍ" للاقتداءَ بها لدى تصديرِ بعض البياناتِ خارج الاتحادِ الأوروبيّ نشر يوم ٥ فبراير ٢٠١٠) 2010/87/UE)[٣٥].

في السِياقِ عينه، صدَرَ الإرشادُ الأوروبيّ عام ٢٠٠٢[٣٦] مُستهدِفاً شركاتِ تقديمِ شبكاتِ الاتصالاتِ العامة والخاصة، والذي بموجبه ينبغي أنْ يكونَ النفاذُ فيها إلى البياناتِ الشخصيةِ بِتفويض شخصيّ للأغراض المُصرّح بها قانوناً، أو أنَّه ينبغي أنْ يكون تخزينُ البياناتِ الشخصيةِ أو نقلها محمياً ضِدّ الإتلافِ العرَضيّ أو غير القانوني أو الضَياع أو التغيير العرَضي، وضد التخزين أو المُعالجة، أو النَفاذ، أو الإفشاءِ غير المُصرح به أو غير القانونيّ.

كما تجدرُ الإشارةُ، إلى "المعاهدةِ الأوروبيةِ معاهدة بودابست لمكافحة الجرائم السيبرانية،

(٣٣) Jump up to: abc"Judgment in Case C-362/14 Maximillian Schrems v Data Protection Commissioner: The Court of Justice declares that the Commissions US Safe Harbour Decision is invalid"(press release) (Press release). Court of Justice of the European Union. 6 October 2015. p. 3.Retrieved 7 October 2015.

(٣٤) عدلت هذه التوصية بموجب التوجيه رقم ٥٨ / ٢٠٠٢ حول حماية الحياة الخاصة والاتصالات الالكترونية ثم بموجب التوجيه رقم ٢٠٠٦/٢٤ حول حفظ البيانات.
European Parliament and the Council of Europe: Directive 2006/24/EC, on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communications networks and amending Directive 2002/58/EC.

(٣٥) 2010l87, Décision de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil [notifiée sous le numéro C(2010) 593] (Texte présentant de l'intérêt pour l'EEE), OJ L 39, 12.2.2010, p5-18.

(٣٦) Directive 2002/19/EC of the European Parliament and of the Council of 7 march2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive

لعام ٢٠٠١[٣٧] التي تنصُّ على التزام الدولةِ، حيث ارتُكِبَت الجريمةُ السيبرانيةُ، بالاحتفاظِ بالبياناتِ الخاصةِ بحركة الاتصالاتِ والكَشفِ عنها إلى الدولةِ التي تطلُبُ هذه البياناتِ.

ولا بُدّ من ذكر الإطارِ التنظيميّ لِعمل المجلسِ الأوروبيّ تاريخ ٢٧ نوفمبر ٢٠٠٨، حول حمايةِ البياناتِ الشخصيةِ[٣٨] في مجال التعاونِ القضائيّ والأمنيّ فيما يتعلق بالبياناتِ الخاصةِ بالشؤونِ الأمنيةِ والعسكريةِ المُتبادلةِ بين دول الاتحادِ.

بِدورهم، توجَّهَ قادةُ القِطاعاتِ الصناعيةِ والتجاريةِ في أوروبا إلى المفوضية الأوروبيّة لإيجاد الإطارِ التشريعيّ المُلائِم لِخدمات الحوسبةِ السحابيةِ[٣٩].

وفي عام ٢٠٠٩، أصدَرَت المُفوضيّة الأوروبية مُدوّنةَ سلوكٍ بشأن الكفاءةِ في استهلاك قواعد البياناتِ للطاقة، ووضعت مجموعةً من التدابيرِ الطوعِيةِ، منها تحقيق الكفاءةِ في تصميم قواعد البياناتِ وتشغيلها[٤٠]. وفي ٢٥ يناير ٢٠١٢، نشرَت المفوضيةُ الأوروبيةُ التعديلاتِ المُقترح إدخالها على "التوجيه الأوروبيّ لحماية البياناتِ"[٤١]، في محاولة لتنسيق الإطارِ التشريعيّ وسائر القوانين المحليةِ المُتعلقة بحماية البياناتِ ضمن دول الاتحاد. وتتضمن التعديلاتُ المُقترحةُ ما يأتي:

* تمكين السلطاتِ التنظيميةِ الوطنيةِ من اتخاذِ إجراءاتٍ ضد الشركاتِ العامِلةِ في الدولِ الأعضاءِ الأخرى في ظُروف مُعيّنة، مع الحق في فرض غراماتٍ تصل إلى ٢ مليون يورو أو في بعض الحالات ٢ في المائةِ من حجم الأعمالِ السنويّ للشركَةِ.
* توسيعُ تعريف البياناتِ الشخصيةِ، بحيث يُغطّي أي معلوماتٍ متصلةٍ بصاحب البياناتِ، وتَشترطُ القواعدُ التنظيميةُ الحصولَ على موافقة صريحةٍ من الفردِ بالسماحِ بحجب البياناتِ.
* تطبيقُ القواعد التنظيمية فيما يتجاوز الاتحاد الأوروبي، بحيث تشمُل كل الدول الأوروبية (بما فيها تلك غير المنضمة إلى الاتحاد الأوروبي) التي تمتلِكُ بياناتٍ شخصية ذات صِلة بمواطني الاتحاد الأوروبيّ.
* يُشترط أنْ تقومَ الهيئاتُ المعنيّة بالإبلاغِ بدون أي تأخير غير مبرر عن أي خرقٍ للبياناتِ، وأن يتمّ ذلك في غضون ٢٤ ساعة من وقوع الخَرقِ
* يُشترط أن تقومَ الشركاتُ المُتحكّمة في البياناتِ بتقييم مدى حِماية البياناتِ وتعيين مسؤولين عن حماية البياناتِ وإبلاغ الأطرافِ الأُخرى بأيّة خروقات.
* يكون للأفراد حقٌّ جديدٌ هو "الحق في النسيان" في ظُروف مُعيّنة ولا يكونوا مُطالبين بعد الآن بِدفع مُقابلٍ للنفاذ إلى بياناتِهم.

---

(٣٧) Convention on Cybercrime (Budapest, 23 November 2001), http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

(٣٨) Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters OJL 350, 30.12.2008.

(٣٩) EU Commission: Industry calls for true digital single market in recommendations on European cloud strategy.

(٤٠) Code of Practice: Protection of personal Data, 2009. https://dataprotection.ie/documents/code%20of%20practice/RevenueCOP.pdf

(٤١) Personal data protection: processing and free movement of data (General Data Protection Regulation) http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2012/0011%28COD%29

* تخضعُ عمليات النقلِ الدولي للبياناتِ إلى إطار تنظيميّ أكثر تفصيلاً ينصُّ على ضماناتٍ يجب تطبيقُها على أَنْ تقومَ السلطاتُ بإجراء فُحوص مُسبقة وزيادة تقييد قُدرة الشركاتِ المُتحكمةِ في البيانات على إبطال هذه الضماناتِ.

وفي مايو ٢٠١٢، نشرَ البرلمانُ الأوروبيّ دراسةً، حدّدَت الطُرق التي ينبغي أنْ يتبنّاها واضعو السياساتِ لتيسير الحوسبة السحابيةِ[٤٢]. وتشملُ هذه الطرقُ التعاملَ مع الثغراتِ المُتصّلة بالتشريعاتِ؛ وتحْسين الشروطِ والأحكامِ لجميع المُستعملين؛ ومعالجة المخاوف والشواغلِ المُتصلة بالأمنِ لدى أصحاب المصلحةِ؛ وتشجيع الأخذِ بالحوسبةِ السحابيةِ في القطاعِ العامِ[٤٣]؛ وتشجيع التوسّع في البحثِ والتطويرِ في مجالاتِ الحوسبةِ السحابيةِ.

قبل الختام، نشير الى أنّ الاتحاد الأوروبي، بصفته إقليماً متكاملاً جغرافيا، اقتصادياً، سياسياً، مالياً، سريع التأثّر بإشكاليات الإجرام الحديث... لكن تبيّن لنا أنّ المجلس الأوروبي يشكّل منذ ١٩٥٠ مختبراً اقليمياً وبوتقة دولية في ما يختصّ بالمواد الجزائية في الأفكار والمبادرات في المسائل الجزائية والمشاكل الإجرامية؛ فصِيغت في إطاره العديد من الاتفاقيات الجزائية لمكافحة هذا الإجرام.

تجسّد اتفاقية Strasbourg لمكافحة تبييض الأموال (١٩٩٠) منهجاً متكاملاً للتعاون في المسائل الجنائية لتعقّب كل الأموال الجرمية المصدر، وليس تلك الناتجة من المخدرات فقط، كما هو نطاق اتفاقية فيينا (١٩٨٨).

كما أنّ كل من اتفاقية القانون الجنائي لمكافحة الفساد (٢٠٠٤)، اتفاقية القانون المدني (٢٠٠٢)، اتفاقية حماية المصالح المالية الأوروبية (١٩٩٥)، البروتوكولات الثلاثة المضافة واتفاقية OCDE لمكافحة رشوة الموظفين العموميين الأجانب (١٩٩٧)... تعبّر عن الاهتمام الأوروبي وعزمه على تجريم منسّق وفاعل وتوفير حد قانونيّ ومعايير إجرائية لعدد كبير من الممارسات الفاسدة.

ختاما، تعدّ اتفاقية مجلس أوروبا في شأن الجريمة السيبرانية Cyber-crime أول اتفاقية تسنّ على الصعيد الدولي لمكافحة الجرائم المعلوماتية.

(٤٢) Cloud computing: A legal maze for Europe / Euractiv, 18/4/2012 - Overview of cloud computing, its benefits and the associated legal issues.http://www.euractiv.com/innovation-enterprise/cloud-computing-legal-maze-europe-linksdossier-511262

(٤٣) DEMOULIN (Marie), SOYEZ (Sébastien): L'archivage électronique dans le secteur public: entre archivage légal et archivage patrimonial, in: L'archivage électronique et le droit (sous la direction: Marie DEMOULIN), CRIDS, Larcier, 2012, Bruxelles, p37 et suiv.