مبادرات الحكومات في حماية الأطفال من أخطار المعلوماتية

العربي بن حجار ميلود ، المجلد العاشر، العدد 3، ديسمبر 2019،
ص ص 391-423

E-ISSN : 2571-9742
P- ISSN: 1112-945X

مبادرات الحكومات في حماية الأطفال من أخطار المعلوماتية: المبادئ والممارسات الناشئة

International law takes precedence over domestic law

ميلود العربي بن حجار

جامعة وهران 1 ، الجزائر

larbibenhadjar.miloud@univ-oran1.dz

تاريخ الإيداع: **2019/09/06** تاريخ القبول: **2019/09/18** تاريخ النشر: **2020/01/31**

الملخص:

أصبحت تكنولوجيات المعلومات والاتصالات (ICT)، وخاصة تقنيات الإنترنت والهاتف المحمول جزءًا لا يتجزأ من حياة الأطفال، و يعتمد المزيد والمزيد من الأطفال عليها للتعلم والمشاركة واللعب والعمل والتواصل الاجتماعي، كما تثبت تكنولوجيا المعلومات والاتصالات أيضًا أنها مفيدة في حماية الأطفال، ويمكن استخدامها للبحث عن المعلومات حول الخدمات وجمع وتوثيق ومشاركة البيانات والإبلاغ عن إساءة الاستخدام. علاوة على ذلك، يمكن أن يكون لتكنولوجيا المعلومات والاتصالات إمكانات هائلة للتغلب على العديد من التحديات، فهي أداة قوية جدًا تفتح الباب أمام العديد من إمكانيات التنمية وأيضًا العديد من الأخطار المحتملة. كما أن الحكومات في جميع أنحاء العالم تعمل بنشاط على تعزيز البنية التحتية للإنترنت، من حيث نشرها واستخدامها في مكان العمل والمدارس والمجتمعات والأسر، ويجب على صانعي السياسات تحديد أفضل السبل لتسهيل الفرص عبر الإنترنت مع تقليل المخاطر المرتبطة بها أو إدارتها، رغم أنه لا تزال هناك صعوبات في تحديد الفرص ومخاطر المعلوماتية التي قد تحمل العديد من المبادرات الجارية وطنيا ودوليا لوضع نظام تنظيمي للبيئة عبر الإنترنت

الكلمات الدالة:

تكنولوجيا المعلومات والاتصالات، المعلومات والبنية التحتية للإنترنت، تكنولوجيا المعلومات والتنمية المستدامة، أمن المعلومات ، تكنولوجيا الهاتف المحمول.

Abstract:

Information and communication technologies and more importantly mobile technologies, internet and social media becomes an integral part of children's lives, more and more children rely upon it for the purpose of learning, sharing, playing games as well as working and socializing with others, however ICT is useful for number of reasons the protection of children , searching for information about

E-ISSN : 2571-9742
P- ISSN: 1112-945X

services, collection of data, documentation, data sharing, dissemination of information and reporting suspicious activity as well as report abuse. Moreover it has an impact if one tends to think of overcoming challenges in addition to that it is powerful tool that opens a door to many of the possibilities of development and potential risks.

Governments throughout the world are working hard in promoting Internet infrastructure, in terms of its use in the workplace, schools, communities, and families and to spread it as well. Policy makers have to find the way to facilitate the chances through the internet and to keep pace with information security risk management on the one hand and technical, scientific and information technology development on the other.

Key Words:
ICT; information internet infrastructure; information technology; sustainable development, information security; mobile technology.

1. مقدمة:

إن الفضاء الرقمي قد سمح للتحديات بالانتشار على نطاق أوسع، والوصول إلى جمهور أكبر بكثير وبسرعة، سواء من حيث إدراك الناس للتحديات ولوجود منصة لتبادل مشاركتهم في هذه الأنشطة، إذ زادت وسائل التواصل الاجتماعي التي سمحت لنا بإظهار أنفسنا وحياتنا اليومية على الإنترنت، كما سعى المستخدمون عبر الإنترنت، وخاصة الأصغر منهم، إلى تقليد وإثارة إعجاب أصدقائهم، لأنه يجعلهم يشعرون أنهم ينتمون إلى مجموعة معينة.ما ساعد ذلك هو انتشار الهواتف الذكية، وكذلك العديد من الأجهزة الأخرى، التي تعمل بالفعل بشكل كامل في الحياة اليومية للأشخاص من جميع الأعمار، إنها أدوات مفيدة للغاية للعديد من الأشياء، ولكنها قد تصبح أيضًا خطيرة جدًا إذا لم يتم استخدامها بشكل صحيح. فحسب اليونيسف لا يزال الأطفال في العالم يواجهون العنف في منازلهم ومدارسهم وعلى شبكة الإنترنت، ولا يزالون مشردون بسبب الصراع والكوارث، كما يواجهون زيادة مخاطر العنف وعمالة الأطفال واستغلالهم، وأكثر من 100 دولة تفتقر إلى أنظمة تسجيل المواليد وهي واحدة من الأدوات الأولى لحماية حقوق الأطفال وسلامتهم[1]، عندما نقول الأطفال على الإنترنت، يعني أن الأبوة والأمومة اليوم تتضمن معرفة إلى أين هم ذاهبون وماذا يفعلون هناك أفضل خط دفاع ضد أي مخاطر كامنة.

E-ISSN : 2571-9742
P- ISSN: 1112-945X

1.1 مشكلة الدراسة: نعلم اليوم أن الإنترنت والهواتف الذكية وغيرها من التقنيات هي أدوات رائعة لجمع المعلومات ومشاركة الموارد والبقاء على اتصال مع الأصدقاء والعائلة وللعثور على أشخاص يشاركوننا اهتماماتنا. في الوقت نفسه، توفر هذه التكنولوجيا الوصول إلى الأطفال والمراهقين بطرق يمكن أن تكون مجهولة المصدر وفعالة للغاية، مما يعرضهم لخطر الأذى من المتسللين عبر الإنترنت والمواد الإباحية والبلطجة عبر الإنترنت والرسائل النصية وغير ذلك من الأخطار، على الرغم من توفر المزيد من الحماية الآن إلكترونيًا لمنع هذه المشكلات، إلا أن كلمات مثل الأمان عبر الإنترنت، و "الأجهزة" هي إضافات حديثة إلى مفرداتنا، نظرًا لاستمرار تغير الأشياء، غالبًا ما يكون الأطفال أكثر ذكاءً من البالغين، بينما يفتقرون إلى تجربة حياتنا حول كيفية التعرف على المشكلات وتجنبها، كما أن برامج الأمان يمكن أن تصبح قديمة بسرعة. حيث ظهرت تحديات ومخاطر كثيرة عبر الإنترنت منها تحدي المد والجزر (Tide Pod challenge)، تحدي زجاجة الوجه(Bottle Flip challenge)، تحدي الحوت الأزرق(Blue Whale challenge)، تحدي # مشاعري (#InMyFeelings challenge)، تحدي مومو(Momo challenge)، وكل يوم تظهر تحديات جديدة على الإنترنت بشكل منتظم وسرعان ما تتكاثر على وسائل التواصل الاجتماعي، وخاصة بين الأطفال والشباب، وهي تتراوح بين إيجابية ومفيدة ومضحكة إلى مخيفة، يحتمل أن تكون ضارة وحتى قاتلة.

2.1 تساؤلات الدراسة: نحاول في هذه الدراسة *طرح التساؤل الرئيسي*: كيف عملت الحكومات على حماية أطفالهم من مخاطر المعلوماتية؟

تساؤلات فرعية: كيف يمكن تعليم الأطفال استخدام الإنترنت بأمان؟ وكيف يمكننا ضمان بقاء الأطفال و الشباب وجميع مستخدمي الإنترنت في أمان؟

3.1 فروض الدراسة: عملت الحكومات على حماية أطفالهم من مخاطر المعلوماتية بتوفير مواقع وأدوات توعوية.

4.1 أهداف الدراسة: الهدف من هذه الدراسة هو الوقوف على واقع الحماية من مخاطر المعلوماتية التي وفرتها الدول المتطورة والسائرة في طريق النمو لأطفالها من أجل نموهم السليم، وإعطاء صورة واضحة عن الجهود المبذولة من طرف الحكومات لتلك الدول.

5.1 منهج الدراسة: من أجل الوصول لنتائج مرضية استخدمنا المنهج الاستدلالي من أجل البرهنة والذي بدأناه بقضايا مسلم بها، وسرنا نحو قضايا أخرى نتجت عنها بالضرورة، أي

E-ISSN : 2571-9742
P- ISSN: 1112-945X

الاتجاه من قضايا بسيطة ثم تركيب بعضها مع بعض حتى يتم الوصول إلى قضايا أكثر تعقيدا، حيث استخدمنا التسلسل المنطقي المنتقل من مبادئ أو قضايا أولية إلى قضايا أخرى تستخلص منها، كون النظام الاستدلالي يقوم على أساس متصل من الموضوعات غير القابلة للتحديد، من أجل تركيب موضوعات جديدة موجودة منطقيا.[2]

2. تجارب لأباء الغرب في كيفية حماية أطفالهم من أخطار المعلوماتية:

أصبحت تكنولوجيات المعلومات والاتصالات (ICT)، وخاصة تقنيات الإنترنت والهاتف المحمول جزءًا لا يتجزأ من حياة الأطفال[3]. ومن الشائع جدًا أن يتلقى الأطفال أول هاتف ذكي لهم خلال 8 أو 9 سنوات، ويمكن تخفيض هذا العمر في بعض الأحيان أكثر قليلاً عندما نتحدث عن الأجهزة اللوحية، ما لا يعرفه الكثير من الآباء والأمهات هو أنه بينما يتم إعطاؤهم أداة قوية جدًا تفتح الباب أمام العديد من إمكانيات التنمية وأيضًا العديد من الأخطار المحتملة[4]. ويعتمد المزيد والمزيد من الأطفال عليها للتعلم والمشاركة واللعب والعمل والتواصل الاجتماعي، كما تثبت تكنولوجيا المعلومات والاتصالات أيضًا أنها مفيدة في حماية الأطفال، ويمكن استخدامها للبحث عن معلومات حول الخدمات وجمع وتوثيق ومشاركة البيانات والإبلاغ عن إساءة الاستخدام. علاوة على ذلك، يمكن أن يكون لتكنولوجيا المعلومات والاتصالات إمكانات هائلة للتغلب على العديد من التحديات التي يواجهها الأطفال الضعفاء في العالم غير المتصل بالإنترنت. على سبيل المثال، بالنسبة للأطفال ذوي الإعاقة، يمكن لتكنولوجيا المعلومات والاتصالات أن تكون بمثابة أدوات قيمة للوصول إلى الخدمات وإتاحة فرص للإدماج الاجتماعي والتواصل والمشاركة[5].

كون الفضاء الإلكتروني واستخدام الأجهزة التكنولوجية بشكل متزايد يوفر العديد من المرافق، خاصة بالنسبة للأطفال والشباب مثل التفاعلات بين الثقافات في جميع أنحاء العالم، والدعم الأكاديمي، تنمية التفكير الشخصي والنقدي، الدعم الاجتماعي واستكشاف الهوية. ومع ذلك، يمكن أن تسبب كل هذه المرافق العديد من المخاطر بالنسبة للأطفال غير المجهزين[6]، فالوصول السهل والخاص في الكثير من الأحيان الذي توفره الإنترنت للأطفال كوسيلة جديدة، يمكن أن ينتشر من خلالها استغلالهم، وسوء المعاملة، والإيذاء الجنسي والعاطفي بشكل عام، فإن الإنترنت يمنح المفترسين إمكانية الوصول الفوري إلى مجموعة كبيرة من الضحايا المحتملين وإغرائهم، ويوفر العديد من الفرص و المزايا للحيوانات المفترسة، حيث

E-ISSN : 2571-9742
P- ISSN: 1112-945X

غرف الدردشة وألعاب لعب الأدوار مثل (World of Warcraft) والعوالم الافتراضية مثل (second life) ومواقع الشبكات الاجتماعية مثل (Facebook) ، تسهل برامج المفترسين من خلال السماح للمشاركين بالبقاء مجهول أو إنشاء هويات مزيفة، وهذا من خلال إخفاء هويتهم الحقيقية ودوافعهم، ويكون المفترسون قادرين على بناء علاقات طويلة الأمد عبر الإنترنت مع ضحاياهم المستهدفين قبل أي محاولة لتعزيز الاتصال الجسدي. وفي الآونة الأخيرة، أصبحت هناك أشكال مختلفة من المضايقات وقضايا أكثر بروزًا للأطفال والمراهقين[7].

وفقا لدراسة أعدتها مجموعة (S2 Group)، وهي شركة متخصصة في الأمن السيبراني، أن 75 ٪ من الآباء والأمهات لم تنفذ أي نوع من الرقابة الأبوية في المحمول الخاص بأطفالهم، هذه النسبة مثيرة للقلق لا يمكن للآباء أن ينسوا دورهم في تعليم وحماية أطفالهم ضد التقنيات الجديدة، يجب عليهم تثقيفهم وإخبارهم عن المخاطر المحتملة وسوء الاستخدام و أفضل طريقة لمنع حدوث ذلك هي حوار الأهل مع الأطفال، يمكن بعد ذلك دعم هذا العمل بتنظيم عدد الساعات التي يمكن استخدامها لمنع بعض الإدمان، أو حتى استخدام أدوات الرقابة الأبوية، والتي يمكن أن تمنع الوصول إلى المحتوى الخطير، فمن المهم بنفس القدر أن تشرح للأطفال الصغار أنهم قاموا بتثبيتها والتي ستوفر لهم الأمان وسيكون لديهم زيادة الوصول إلى المزيد من استخدامات الجهاز، نظرًا لأن الطفل الذي يخفي كل هذه المعلومات، سينتهي به الأمر إلى محاولة إزالته بالقوة، ويجب عليهم فهم الخطر في حالة الوصول إلى هذا المحتوى من خلال وسائل أخرى [8].

يحاول الآباء الغربيون حماية أطفالهم من مخاطر المعلوماتية عن طريق[9]:

- بدء عملية مناقشة الأمان عبر الإنترنت مع أطفالهم في سن مبكرة، إذ ربما لا يزالون يستخدمون الكمبيوتر معهم وليس بشكل مستقل، وهذا يوفر فرصة لتسليط الضوء على حقيقة أن عالم الإنترنت يوازي العالم الحقيقي وأن هناك أشياء آمنة وغير آمنة، ومع تقدمهم في السن والبدء في عمل الأشياء بشكل مستقل، قم بتوسيع الدائرة، على سبيل المثال، إذا سمحت لهم ببدء حساب مع (Club Penguin) أو (Moshi Monsters)، ساعدهم في إنشاء كلمة مرور معقولة وشرح لماذا يجب عليهم استخدام كلمات مرور مختلفة لكل حساب والنتائج المحتملة لعدم القيام بذلك.

E-ISSN : 2571-9742
P- ISSN: 1112-945X

- تذكيرهم أن الإنترنت لا يزال هو العالم الحقيقي، ويحتاج المراهقون أن يتذكروا أن كل ما يفعلونه عبر الويب يتم التقاطه إلى الأبد ويمكن أن يعود ليطاردهم.
- مسح أجهزتهم ضوئيا بحثا عن البرامج الضارة والتأكد من بقائها مصححة تماما.
- تعلمهم الحذر من الغرباء الذين يحملون هدايا، حيث لا تسمح لهم بفتح حزمة بريد إذا لم يعرفوا من أرسلها ولا بفتح مرفقات البريد الإلكتروني غير المرغوب فيها، خاصة وأن شعورهم بالفضول أكثر تطوراً وأن شعورهم بالحذر أقل نضجًا، لا نتوقع أن يتصرف الأطفال على الإنترنت بشكل مختلف كثيرًا عن الواقع الفعلي، ولذا عليك أن توضح لهم أن المتسللين هم نوع من المجرمين ينتشرون في منزلك عبر الكمبيوتر بدلاً من النافذة.
- معرفة ماذا يكتبون على الإنترنت فبمجرد كتابة شيء ما لا يمكنه حذفه، وعلى الطفل أن يكون حذراً فيما يفعله ويقوله.
- عدم التصفح أبدًا تحت أي ظرف من الظروف، نحن نشير إلى أن نكون منفتحين حول مفهوم المحتوى غير المناسب ووجود أشخاص سيئين، حيث اعتدنا أن نرغب في أطفال حكيمين في الشوارع، نحتاج الآن إلى أطفال حكيمين على الويب.
- محاولة أن يكون متيقظًا ويراقب ما يستطيع من خلال مراقبة تقارير الائتمان الخاصة بهم.
- تثقيفهم مبكرا من خلال مشاركتهم بانتظام المواقع التي تستخدمها، مع مراجعة جميع التنزيلات والتطبيقات وبهذه الطريقة يمكن للأب مراقبة إعدادات الأمان والإصدار على أنها آمنة ومناسبة للاستخدام.
- قضاء الوقت معهم لإظهار أنهم أكثر جدارة بالثقة عندما يتعلق الأمر بالإنترنت.
- التأكد من أن أطفالك لا يقبلون سوى الرسائل ويقبلون طلبات الأصدقاء والاتصال بأشخاص يعرفونهم، اطلب رؤية أجهزتهم النقالة بشكل دوري، ولكن إذا لم يكن هناك شيء آخر، فابحث عن التطبيقات المثبتة، وقم بإجراء جرد ذهني، وإذا لم يكن الوالد على دراية بالتطبيق، فانتقل عبر الإنترنت وإجراء التحقيق، وبهذه الطريقة، على الأقل تعرف أنواع خدمات التواصل الاجتماعي التي يستخدمها طفلك، يجب عليك على الأقل الاشتراك في هذه الخدمة لمعرفة ما يدور حوله.

E-ISSN : 2571-9742
P- ISSN: 1112-945X

- تشجيعهم على إخبار الآباء إذا ما قاموا بالنقر فوق شيء لا يحبون مظهره.
- أن يكونوا حذرين فيما يفضحون وأن هويتهم وكل ما يصاحبها ثمين، ومن المهم التفكير في استخدام اسم مستعار، وعدم الكشف عن عمر الشخص أو جنسه، والحد من تحديد معلومات بعض تفاعلاتهم عبر الإنترنت.
- التأكد من أن الأمن السيبراني هو عنصر مهم، وكل ما يتعلمه الأطفال ويقومون به على أجهزة الكمبيوتر الخاصة بهم وعبر الإنترنت حتى يصبحوا خبراء في الأمن، كما عليك تذكيرهم بانتظام بأنه يمكن لمواقع الويب إعادة التوجيه إلى مواقع أخرى دون أن تكون على علم، ومشاركتها عند تثبيت التصحيحات، حتى يدركوا أهمية ضمان تحديث الأنظمة.
- تثقيف الأطفال حول مخاطر المعلوماتية باستخدام مواد أو صور، مثل رسوم كاريكاتير الويب لتوضيح هذه النقطة حيث من المرجح أن يستمعوا إليها. علّم الأطفال أن يراجعوك أولاً قبل تغيير خطتهم المتعلقة بالأنشطة عبر الإنترنت - بما في ذلك قبل وضع أي معلومات شخصية عبر الإنترنت عن طريق ملء الاستبيان أو التسجيل على موقع ويب أو الانضمام إلى مجموعة محادثة أو إرسال صورة ،أو أين يعيشون، وأين يذهبون إلى المدرسة، أو أسمائهم، أو رقم هاتفهم، أو اسمك، أو مكان عملك، أو أسماء أصدقائهم أو أسرهم أو مدرسيهم، أو الفريق الرياضي، أو الجيران، أو المدينة.
- مناقشة استخدامهم لوسائل التواصل الاجتماعي كونها مكان جيد للبدء، بما أن استخدام هذه المنصات أصبح واسع الانتشار الآن، من المهم وضع طرق لمنع المحتوى غير المناسب والتحدث مع أطفالك حول مخاطر تكوين علاقات مع الغرباء عبر الإنترنت، وكذلك أهمية منع صنع المعلومات الشخصية عامة.
- إعطاء للطفل فكرة عن ماهية مخاطر المعلوماتية، حيث أظهرت دراسة حديثة أن الآباء يشترون الآن هواتف ذكية لأطفالهم عندما يكون عمرهم أقل من 5 سنوات، إن الاستخدام المبكر للهواتف الذكية والأجهزة اللوحية يزيد من خطر الإصابة بالبرامج الضارة والاحتيال عبر الرسائل النصية القصيرة، مما يجعل العديد من الضحايا المستخدمين الذين ما زالوا يتعلمون القراءة فقط.

E-ISSN : 2571-9742
P- ISSN: 1112-945X

- اتباع الطفل لنفس القواعد التي يتبعها في العالم الحقيقي، إذا لم تكن متأكدًا من شيء ما أو شخص ما، اسأل والديك أو شخص بالغ مسؤول آخر، وإذا حدث أي شيء "غير عادي" عند استخدام جهاز الكمبيوتر الخاص بك، فأخبر والديك، وإذا أخبرك أي من أصدقائك بكيفية تجاوز مرشحات المحتوى وحواجز تثبيت التطبيق، لا تفعل ذلك فقط اذهب لوالديك وتحدث معهم حول ما تحتاجه.
- الأمن والخصوصية: إن نسبة 57 % من الاطفال والشباب يعانون من خطر مشاركتهم لمعلوماتهم مع أجانب، لهذا يمكن تعيين إعدادات الخصوصية على منصات الوسائط الاجتماعية للمساعدة في تصفية من يرى معلوماتك وصورك ومقاطع الفيديو الخاصة بك، من المهم دائمًا التفكير فيما يجب مشاركته ومع من إذا لم تكن إعدادات الخصوصية آمنة، يعد الأمان من الأنظمة الأساسية والقنوات التي نستخدمها أمرًا ضروريًا أيضًا، يمكن أن تسمح الأنظمة غير الآمنة بانتهاك الخصوصية، إن بناء إنترنت أفضل يعني مشاهدة ما تشاركه والالتزام بخصوصية الآخرين، هذا يعني أيضًا معرفة ما إذا كان يمكن الوثوق بالمنصات والقنوات التي تستخدمها للحفاظ على أمان معلوماتك[10].
- ساعد الأطفال على فهم أن استخدامهم للتكنولوجيا هو امتياز وليس حقًا وأن التسلط عبر الإنترنت أو أي عدوان إلكتروني آخر يخالف قيمك، كون لديهم قواعد ونتائج واضحة لإساءة استخدام التكنولوجيا الضارة بالآخرين أو محفوفة بالمخاطر لأنفسهم، وتعزيز فكرة أن تكون مواطنا رقميا جيدا، إذ توفر اتفاقية المواطنة والسلامة الرقمية الخاصة بـ (Kid power) أداة مفيدة لإبرام عقد واضح مع أطفالك[11].

لقد أثبتت الدراسات أن أولياء الأمور هم أفضل خط دفاع حقيقي في كثير من الأحيان للحفاظ على أمان الأطفال والمراهقين والشباب، عليهم أن يكونوا على دراية بالمنصات التي يستخدمها أطفالهم، يعد حساب الوسائط الاجتماعية أو الهاتف الذكي هو الوقت المناسب لوضع القواعد الأساسية وإجراء محادثات، إذا كان لديهم بالفعل واحدة من الخطط للبدء في التحدث معهم حول شخصيتهم الرقمية اليوم. وعندما يكون الأطفال في غرفة نومهم على كمبيوتر محمول أو هاتف ذكي مع إمكانية الدردشة عبر الفيديو، أعرف أن هذه وصفة لكارثة،

E-ISSN : 2571-9742
P- ISSN: 1112-945X

أطلب منهم القيام بالواجب المنزلي فقط في غرفتهم ووسائل التواصل الاجتماعي في غرفة العائلة لهذا راقب نشاطهم[12].

3. الأطفال والمعلوماتية بالغرب بين المنفعة والضرر:

أكثر من 175.000 طفل يتصفحون الإنترنت للمرة الأولى كل يوم - طفل جديد كل نصف ثانية، وما يحدث في عالم الإنترنت هو انعكاس للمجتمع ككل، قد يتعرضون للعنف والاستغلال والإيذاء في منازلهم حيث يتعرض 80 % من الأطفال وحتى سن 18 للاعتداء الجنسي والاستغلال، وتعكس المدارس والمجتمعات المحلية العنف الذي قد يواجهونه عبر الإنترنت، وإساءة استخدام الأطفال عبر الإنترنت تأخذ أشكالًا متعددة، الجناة قد ينتجون ويوزعون ويستهلكون مواد الاعتداء الجنسي على الأطفال؛ أي إلحاق الأذى بالأطفال من خلال البث المباشر، و يسير مرتكبو الجرائم الجنسية للتكييف بسرعة مع أحدث التقنيات لارتكاب جرائم ضد الأطفال، إن بناء إنترنت أفضل يعني إدراكك لهذه الإساءات، ودعم المستخدمين الذين قد يتعرضون للخطر[13].

إن اكتشاف الجرائم الخطيرة المرتكبة ضد الأطفال في السنوات الأخيرة، لا سيما العنف الجنسي، ووجود شبكات الاستغلال الجنسي للأطفال وإساءة معاملتهم، لا تعرف أي حدود سواء كانت جغرافية أو ثقافية أو اجتماعية، والتي ساعدت بلا شك في تخفيف المعايير الأخلاقية وتزايد عدم المساواة، وهذا أدى إلى وعي مؤلم بهذه المشكلة في أوروبا، حيث أدى اكتشاف الجرائم الخطيرة المرتكبة ضد الأطفال، إلى إثارة وعي مؤلم بهذه المشكلة، وهي آلام تتطلب اتخاذ إجراءات حازمة ومشاورات وتعاون حقيقيين على المستوى الأوروبي، وقاد لجنة الشؤون الاجتماعية والصحية والأسرية إلى إجراء مناقشة طارئة في سبتمبر 1996 واتخاذ القرار 1099 (1996) بشأن الاستغلال الجنسي للأطفال، وعلى هذا الأساس تم تأسيس مشاريع منها مجلس أوروبا (The Council of Europe's) والغرض منه هو تعزيز سيادة القانون وحماية حقوق الأفراد، كما هو مفهوم في جميع أنحاء القارة. يتمثل المبدأ الأساسي لهذا "النموذج الأوروبي" في الحماية الفعالة لأضعف أفراد المجتمع وخاصة الأطفال[14].

يجب القول إن الاتفاقية الأوروبية لحقوق الإنسان لا تحمي حقوق الأطفال على وجه التحديد إلا في الحالات التي أيدتها فيها المحاكم على أساس حماية الحياة الأسرية. وبالمثل، فإن الاتفاقية الأوروبية المتعلقة بممارسة حقوق الطفل، التي فتحت للتوقيع في 25 كانون الثاني /

E-ISSN : 2571-9742
P- ISSN: 1112-945X

يناير 1996، تحكم وصول القاصرين إلى المحاكم والتمثيل القضائي ولكنها لا تتضمن أي أحكام بشأن الحقوق الموضوعية التي يمكن منحها للأطفال وضمانها قانونًا، حيث لا تزال أوروبا بحاجة إلى تطوير ثقافة حقيقية لحقوق الطفل، إذ يحتاج الأطفال إلى حماية خاصة بسبب ضعفهم وقدرتهم الأقل تطوراً على تقييم المخاطر المختلفة والتي يمكن للكبار تقييمها، مثل الاعتداء الجنسي أو الاغتصاب أو الدعارة أو المواد الإباحية أو زنا المحارم أو سوء المعاملة، وهناك حاجة إلى وضع اتفاقية لمجلس أوروبا تنص على تبادل المعلومات ذات الصلة وإتاحة الإدانات السابقة في واحدة أو أكثر من الدول الأعضاء في المنظمة من قبل المحاكم الوطنية [15].كما تم إطلاق الإصدار الثالث من دليل الأبوة الرقمية لفودافون (Vodafone's) والذي يتضمن بحثًا يلقي الضوء على دور التكنولوجيا الرقمية في الحياة الأسرية الحديثة. تشير البيانات - التي تم جمعها بعد استبيان 1500 من أولياء الأمور و 500 شاب - إلى أن معظم الآباء والأمهات والأطفال يعتقدون أن حياتهم العائلية قد أثرت عليها التكنولوجيا، وأن أكثر من تسعة من كل 10 أطفال يشعرون بأن لديهم المزيد من الفرص بفضل التكنولوجيا، كونها تشجع على الروابط العاطفية الأقوى داخل العائلات خصوصا إذا كنت في بلدان مختلفة، فلن تضطر إلى الانتظار لأسابيع حتى تصل الرسالة، يمكنك فقط الاتصال عبر (Skype) أو(FaceTime). [16]

لكن ليس الكل يتفق بالضرورة على أن هناك حاجة إلى كبح جماح الاستخدام الرقمي للشباب؛ في الواقع، هناك حجة مفادها أن السماح لهم بتطوير حكمهم من خلال التجربة والخطأ أمر مهم، كان هذا هو الرأي الذي طرحه كالوم نيجوس-فانسي (Callum Negus-Fancey) من أخصائي الدعوة في مجال العلامة التجارية (Let's Go Holdings) أن تدرس كيفية إدارة المخاطر هي مهارة حياة مفيدة للغاية، وقد وافق لينينجتون (Linnington) على أنه من المهم تشجيع الشباب على استخدام مهارات التفكير النقدي التحليلي لتقييم الآثار المترتبة على استخدام تقنيات معينة. وقد ناقش (Negus-Fancey) أن التكنولوجيا قد منحت الأطفال مزيدًا من الاستقلالية وسمحت بالتسوية مع الوالدين؛ ويمكن للمراهق الذي لديه هاتف محمول أن يرن إلى المنزل لتخفيف أي مخاوف بشأن سلامته بدلاً من الاضطرار إلى العودة إلى المنزل بفرض حظر تجول صارم في هذه الحالة، ومن من المؤكد أن البيانات المستقاة من الأبحاث الجديدة التي أجرتها شركة فودافون تدعم ذلك: قال 95٪ من المراهقين للباحثين إنهم

E-ISSN : 2571-9742
P- ISSN: 1112-945X

يشعرون بالأمان أكثر عندما يغادرون منزلهم بهواتفهم المحمولة، هذا لا يعني أنه لا توجد أسئلة صحيحة يجب مراعاتها حول استخدام التكنولوجيا داخل العائلات[17].

يمكن إرجاع المخاوف العامة التي تحيط بتعرض الأطفال لوسائل الإعلام إلى النهاية القرن العشرين في الولايات المتحدة الأمريكية، وقد ركز الباحثون فيه على مقدار الوقت الذي يقضيه الأطفال مع التكنولوجيات الجديدة، ثم انتقلوا إلى محاولات تحديد ما يتعرض له الأطفال من خلال استخدام التقنيات الجديدة، و في النهاية البحث عن الآثار السلبية لهذا الاستخدام، حيث وجدوا أنه كلما زاد تعرض الأطفال للإعلام زادت الآثار السلبية، وقد واصل الباحثون محاولة تحديد مقدار الوقت الذي يقضيه المراهقون في ظل التقنية الحديثة ومع ذلك، قد يكون الأمر أكثر صعوبة، ويرجع ذلك في الجزء الكبير منه إلى القابلية المتزايدة للتكنولوجيا مثل الهواتف الذكية والأجهزة اللوحية وقدرات الاتصال اللاسلكي المتنامية. هذه الأنواع من الدراسات تسعى فقط لتحديد مقدار التعرض لمختلف أشكال وسائل الإعلام والتكنولوجيا، دون دعم فكرة أن التعرض المتزايد ضار.[18] لهذا يوصي أطباء الأطفال الآن بأن نضع قيودًا قوية على مقدار "وقت الشاشة" الذي أمام الأطفال سواء جهاز كمبيوتر أو هاتف محمول أو جهاز ألعاب أو تلفزيون حتى يتوفر للأطفال وقت كافٍ للنوم أو اللعب النشط، نزهات، وغيرها من الأنشطة الاجتماعية والتعليمية في العالم الحقيقي[19].

كما أن هناك العديد من الدراسات التي تحاول تحديد ما إذا كانت هناك علاقة بين استخدام الأطفال وسائل الإعلام والسمنة، حيث تعتبر السمنة عند الأطفال مصدر قلق لعدة أسباب، بما في ذلك الزيادة الملحوظة في معدلات السمنة لديهم في السنوات العشرين الماضية، والعديد من الآثار الصحية السلبية بما في ذلك زيادة خطر الإصابة بمرض السكري و ارتفاع ضغط الدم، وقد أوضحت العديد منها أن استخدام وسائل الإعلام يسهم في وباء السمنة في جميع أنحاء العالم، وقد خلص الباحثون إلى أن تقليل مقدار وقت مشاهدة التلفزيون يؤدي إلى صحة أكثر[20].زيادة على ذلك يمكن أن يؤدي انفتاح الإنترنت إلى جانب الفجوة الرقمية بين الأطفال والآباء ومقدمي الرعاية والمدرسين إلى تعرض الأطفال لضرر على الإنترنت، مما قد يؤثر سلبًا على نموهم الشخصي ورفاهيتهم، وينطبق هذا بشكل خاص على البلدان المنخفضة والمتوسطة الدخل حيث تكون الفجوات في الحماية الشاملة للأطفال أكبر، ومستويات الإلمام بالقراءة والكتابة الرقمية بين الآباء ومقدمي الرعاية أقل، تشمل الأمثلة على المخاطر المحتملة

E-ISSN : 2571-9742
P- ISSN: 1112-945X

التعرض لمحتوى مزعج أو ضار مثل الصور العنيفة والبلطجة الإلكترونية[21]، والتي تكون عادة في شكلين: العلنية والسرية، التنمر العلني ينطوي على عدوان جسدي، مثل الضرب والركل والدفع واللمس الجنسي، يمكن أن يكون مصحوبًا بالبلطجة السرية، التي يتم فيها استبعاد الضحايا من مجموعات الأقران، والمطاردة، والتحديق، والتهديد اللفظي، والمضايقة، يمكن أن يكون التنمر السري عشوائي أو تمييزي، ويمكن أن يشمل المضايقات اللفظية التي تتضمن الإهانات العنصرية أو الجنسية أو المثلية الجنسية[22]، والتماس الجنسي ("الاستمالة عبر الإنترنت") وتداول مواد الاعتداء الجنسي على الأطفال وإساءة استخدام البث المباشر، لذلك من المهم إقامة توازن بين الفرص والمخاطر التي تجلبها تكنولوجيا المعلومات والاتصالات وفهمها بشكل أفضل ما الذي يجعل بعض الأطفال معرضين بشكل خاص لخطر الأذى ، بحيث يمكن استهداف استراتيجيات الحماية بفعالية[23].إذ يكشف البحث الأولي أنه في كندا، 99٪ من المراهقين يستخدمون الإنترنت بانتظام؛ 74٪ من الفتيات اللائي تتراوح أعمارهن بين 12 و 18 عامًا يقضين وقتًا أطول في غرف الدردشة أو الرسائل الفورية أكثر من القيام بواجب منزلي، حيث واحد من كل سبعة عشر طفلاً مهدد على الإنترنت؛ وشاب من كل أربعة شباب تتراوح أعمارهم بين 11 و 19 عامًا مهدد بالكمبيوتر أو الهاتف الخلوي، وهذا ما يجعلهم مهددين بالبلطجة السيبرانية وهو تنوع خفي وسري من التنمر اللفظي والكتابي، يتم نقلها من قبل المراهقين من خلال الوسائط الإلكترونية مثل الهواتف المحمولة، والمواقع الإلكترونية، وكاميرات الويب، وغرف الدردشة، والبريد الإلكتروني ينشئ التلاميذ ملفات تعريف شخصية عبر الإنترنت (مثل Xangas و MySpace) حيث يمكنهم سرد زملاء الدراسة الذين لا يحبونهم، و(Xanga) و (MySpace) هما موقعان للشبكات الاجتماعية يمكن للتلاميذ من خلالها إنشاء ملفات تعريف شخصية، تجمع ملفات التعريف هذه بين سجلات الويب والصور والصوت والفيديو والرسائل الفورية ولوحات النشرات والقدرات التفاعلية الأخرى. يمكن أن تتخذ البلطجة الإلكترونية شكل صور جنسية (يتم إرسالها عبر البريد الإلكتروني بثقة إلى الأصدقاء)، والتي يتم تغييرها وإرسالها إلى جماهير غير محدودة بمجرد توتر العلاقات[24].

4. مبادرات الحكومات والمنظمات في تنظيم الاتصال والمحتوى والحماية من مخاطر المعلوماتية للأطفال:

E-ISSN : 2571-9742
P- ISSN: 1112-945X

الحكومات في جميع أنحاء العالم تعمل بنشاط على تعزيز البنية التحتية للإنترنت، من حيث نشرها واستخدامها في مكان العمل والمدارس والمجتمعات والأسر، ويجب على صانعي السياسات تحديد أفضل السبل لتسهيل الفرص عبر الإنترنت مع تقليل المخاطر المرتبطة بها أو إدارتها، رغم أنه لا تزال هناك صعوبات في تحديد الفرص ومخاطر الإنترنت التي قد تحمل العديد من المبادرات الجارية وطنيا ودوليا لوضع نظام تنظيمي للبيئة عبر الإنترنت[25].

لهذا نقدم المبادرات والمجهودات المبذولة من طرف بعض حكومات العالم في حماية الأطفال من مخاطر المعلوماتية:

1.4. حكومات أوربا:

أطفال الاتحاد الأوروبي يتعرضون لمخاطر الإنترنت منها مخاطر الاتصال، وخاصة الاستمالة عبر الإنترنت و نشاط الاستغلال الجنسي للأطفال، توزيع صور الاعتداء الجنسي على الأطفال أو التهيؤ للطفل على الإنترنت من أجل الاعتداء عليه جنسيا وهذا دوليا يعتبر غير مقبول، والحلول التشريعية عموما هي فقط لظروف عالية الخطورة، لأن تأثيرها هو تقييد الحريات من خلال تكوين مجموعة أوسع من الأعمال غير القانونية مما سيؤدي حتما إلى ضرر، يقوم الأطفال بإجراء العديد من جهات الاتصال عبر الإنترنت وينتج عن ذلك مواجهات ضارة، وإن كانت هذه قد تكون كارثية لضحاياهم. في الواقع، فإن معظم الاتصالات عبر الإنترنت تحمل في بعض الاحيان تجارب إيجابية للأطفال، ذات قيمة كجزء من "حرية التجمع" .تعمل الحكومات والمنظمات الغربية على نطاق واسع على إيجاد الحل المفضل لتحديات تنظيم الإنترنت وهذا ما يسمى *بالتنظيم الذاتي*، وهذا يتطلب التعاون عبر مجموعة غير متجانسة من الأجهزة والبرامج والمحتوى ومقدمي الخدمات، إلى حد كبير من القطاع الخاص ولكن بما في ذلك القطاع العام الكبير، في حين أن هذه العملية الديناميكية للتنظيم لديها بعض المزايا، والتنظيم الذاتي يخدم المصالح الطويلة الأجل للأطفال[26]. شريطة أن يكون هذا التنظيم الذاتي فعالًا أو شفافًا في جهوده، ثم "نحن الجمهور" (من المفترض) أن ندعم حرية إختيار الخدمات التي تدعم بشكل أفضل ميزان الفرص والمخاطر المطلوبة، ولكن إذا كان لم يتم تأسيس فعالية و/ أو شفافية التنظيم الذاتي، يمكن إيجاد بدائل تنظيمية وتشمل العلاقة بين التنظيم والرقابة الاجتماعية[27].

E-ISSN : 2571-9742
P- ISSN: 1112-945X

لهذا تم إطلاق "برنامج الإنترنت الأكثر أمانًا" (The Safer Internet Program) لأول مرة في عام 1999، وهو مصمم لتثقيف المجتمع الأوروبي حول أمان الإنترنت، مع التركيز على المخاطر التي يتعرض لها الشباب مثل (محتوى غير قانوني، السلوك الضار (مثل الاستمالة والبلطجة)، تعزيز بيئة أكثر أمانا، زيادة الوعي)، يجب إبلاغ الشباب وأولياء الأمور ومقدمي الرعاية والمعلمين بالمخاطر المحتملة التي قد يواجهها الصغار عبر الإنترنت، كما يجب أن تكون محاربة المحتوى غير القانوني والضار والسلوك عبر الإنترنت إحدى الأولويات[28].

كما توفر الاستراتيجية الأوروبية لإنترنت أفضل للأطفال (The European Strategy for a Better Internet for Children) مجموعة من التدابير التكميلية، تتراوح بين التمويل والتنسيق والتنظيم الذاتي، حيث أنه في ماي 2012، تم وضع هذه الاستراتيجية لتزويد الأطفال بالمهارات والأدوات الرقمية التي يحتاجونها والاستفادة بشكل كامل وآمن من الاتصال بالإنترنت، كما تهدف إلى فتح إمكانات السوق للمحتوى التفاعلي والإبداعي والتعليمي عبر الإنترنت، كما تقترح الاستراتيجية سلسلة من الإجراءات مجمعة حول الأهداف الرئيسية التالية:[29]

- تحفيز إنتاج محتوى إبداعي وتعليمي وتشجيع التجارب الإيجابية عبر الإنترنت للأطفال الصغار؛
- زيادة الوعي والتمكين بما في ذلك تدريس المعرفة الرقمية والسلامة عبر الإنترنت في جميع مدارس الاتحاد الأوروبي؛
- خلق بيئة آمنة للأطفال من خلال إعدادات الخصوصية المناسبة للعمر، والاستخدام الأوسع للضوابط الأبوية والتصنيف العمري وتصنيف المحتوى ؛
- مكافحة مواد الاعتداء والاستغلال الجنسي على الأطفال عبر الإنترنت.

تجمع الاستراتيجية بين المفوضية الأوروبية والدول الأعضاء مع مشغلي الهواتف المحمولة ومصنعي الهواتف ومقدمي خدمات الشبكات الاجتماعية لتقديم حلول ملموسة لإنترنت أفضل للأطفال[30]، إذ أن المفوضية الاوربية تقوم ببعض التقييم المستقل والمراقبة، وتشمل الأمثلة إطار الهاتف الأوربي وقدرة وفعالية الادوات على التصفية المحلية، حيث تم رصد سنة 2003 أكثر أمانا لمبادئ الربط الاجتماعي الشبكي للاتحاد الأوربي، ولكن الشبكات الاجتماعية والتي مقرها الو.م.أ والمجلس البريطاني المكلف بحماية الأطفال من الإنترنت (UKCCIS) توصلوا إلى اتفاق بشأن المراقبة المستقلة لقواعد السلوك أو التوجيه[31].

E-ISSN : 2571-9742
P- ISSN: 1112-945X

إذ تعمل الاستراتيجية الاوربية بمهامها بشكل رئيسي من خلال تنفيذ مرفق توصيل أوربا (Connecting Europe Facility)، وهي أداة التمويل المشتركة للبنية التحتية عبر أوروبا في قطاعات النقل والاتصالات والطاقة، واقترحت المفوضية الأوروبية سلسلة من المبادئ التوجيهية للاتصالات تغطي أهداف وأولويات البنية التحتية للخدمة الرقمية (Digital Service Infrastructures) وشبكات النطاق العريض من أجل توفير إنترنت أفضل للأطفال، إذ في فترة البرمجة الحالية، تبلغ ميزانية (Connecting Europe Facility) حوالي مليار يورو ، منها 870 مليون يورو مخصصة لبنى الخدمات الرقمية (Digital Service Infrastructures) التي تقدم خدمات عبر الشبكات للمواطنين والشركات والإدارات العامة، والباقي هو لشبكات الاتصال، بالنسبة للفترة 2021-2027، اقترحت المفوضية ميزانية قدرها 3 مليارات يورو، تركز معظمها على جوانب الاتصال، والتي لا تزال خاضعة لاتفاق بشأن ميزانية الاتحاد الأوروبي الشاملة على المدى الطويل[32]. وكذلك من خلال برامج أخرى مثل (H2020)[33].

يشمل ذلك أيضا تخطيط المدن في سياق تخطيط البيئة، حيث لا تفتح ملاعب الأطفال على الطرق الرئيسية ومحلات الجنس ولا تقع بجوار المدارس، ويتم تنظيم المناطق التجارية بشكل مختلف عن تلك السكنية، كما يتم تعليم الأطفال كيفية التعامل مع الغرباء أو السفر حيثما يحتاجون للذهاب أو مع من يمكنهم اللعب بحرية، ومن المثير للاهتمام هو التوازن في التنظيم[34].علاوة على تحديات إنفاذ القانون الدولي، والذي يعقد المهمة التنظيمية للحد من مخاطر الاتصال للأطفال ، لأنه لا يمكن التأكد مسبقًا من أي جهات اتصال إن كانت حميدة أو ضارة، كما أن الأبحاث لم تحدد حتى الآن الأطفال المعرضين للخطر بشكل خاص، و هل من الأفضل تخويف الوالدين التحقق من الاتصالات الشخصية لأطفالهم، أو محاولة تعليم الأطفال الوسائل التقنية المعقدة لحماية خصوصيتهم، أو لضمان موقع "الإبلاغ عن إساءة[35]".

كما أجرت مؤخرا مؤسسة(T.I.M) أول بحث لها مع (Jong & Je Wil Wat) ، تم تنظيم جلسة عمل مدتها ثلاث ساعات مع مجموعة من 15 شابًا تتراوح أعمارهم بين 13 و 18 عامًا، لقد أظهرت أن الشباب الذين شملهم الاستطلاع يعرفون العديد من التحديات عبر الإنترنت، ويميزونها على أساس تأثيرها ومستوى الخطر، وقد تم العثور على هذه التحديات عبر الإنترنت لتندرج في ثلاث فئات[36]:

- تحديات بريئة وغير ضارة مثل التحدي المتمثل في الزجاجة (Bottle flip challenge).

E-ISSN : 2571-9742
P- ISSN: 1112-945X

- التحديات التي تبدأ ببراءة، ولكنها قد تنتهي بشكل خطير، مثل تحدي القرفة (Cinnamon challenge).
- التحديات التي تشكل خطورة واضحة منذ البداية، مثل تحدي مومو(Momo challenge).

ذكر الشباب أن (YouTube) و (Reddit) و (Facebook) و (Instagram) و (Dumpert)و (Twitter) كقنوات للتحديات عبر الإنترنت، لقد أبلغوا عن مشاركتهم فيها لعدة أسباب[37]:

- **التوتر و/أو الإحساس** - العنصر الخطير للتحدي يجعل المشاركة فيهما جذابة و "مسببة للإدمان" تقريبًا.
- **الفضول** - تجربة شيء جديد.
- **تعزيز الصداقات** - مشاركة الأصدقاء ومن ثم الشعور "بالانتماء".
- **زيادة شعبيتها** - الحصول على انتباه الآخرين ، في شكل المزيد من المشاهدات، الإعجابات والمتابعين على وسائل التواصل الاجتماعي.

1.1.4. ألمانيا:

عملت حكومة ألمانيا على بناء حدائق الأطفال المحاطة بجدران أو بوابات كانت أكثر نجاحًا، لا سيما بين الأطفال الأصغر سنا على سبيل المثال، البوابة الألمانية (The German portal FFFIN(fragFinnتتصل بـ 4000 موقع و تستخدم على نطاق واسع من قبل الأطفال[38].

كما نجد المكتب الفيدرالي الألماني لأمن تكنولوجيا المعلومات (BSI (German Federal Office of Information Technology Security) وهو موقع حكومي يقدم التدريب على الاستشارة والمواد المتعلقة بالبروشورات حول السلامة الإلكترونية، يغطي المكتب الكثير من الموضوعات المختلفة التي تتناول الأمن السيبراني في مجال الاستشارة الإلكترونية ، يقدم المكتب ورش عمل (لا سيما فيما يتعلق بأمن تكنولوجيا المعلومات)[39].وأيضا حملة النقر الآمن (Klicksafe) التي تعمل على إظهار المخاطر المختلفة لتصفح الإنترنت وتساعد الجمهور المستهدف الآباء والأساتذة على حماية أنفسهم من الجرائم الإلكترونية بتعليمهم فهم المخاطر والقضايا منها[40]: حماية البيانات، الاتصالات السيبرانية (الدردشة ، البريد الإلكتروني ، البريد المزعج ، الشبكات الاجتماعية ، البلطجة)، ألعاب الكمبيوتر والإدمان، المواد الإباحية، التطرف اليميني، تصوير العنف، التعرض لاضطرابات الأكل، تزوير.

E-ISSN : 2571-9742
P- ISSN: 1112-945X

أما نصيحة الشرطة (polizei – beratung.de) هي صفحة لحملة من قبل الشرطة الألمانية (الفيدرالية والدولة) لمنع الجريمة، ولتحذير وحماية الجمهور (بالغون- أطفال- كبار السن) حول العديد من أنواع الجرائم والجرائم الإلكترونية بشكل خاص، الهدف هو زيادة الوعي بممارسات الإنترنت الآمنة وتغطي هذه الحملة ميدان[41] : التجارة الإلكترونية، التصيد، فيروس وأحصنة طروادة، مخاطر مجانية ، تحميل، تزوير.بينما حملة الرابطة الفيدرالية لحقوق المستهلك (Federal Association of Consumer Rights)، والتي كانت تحت شعار متصفحي الإنترنت لديهم حقوق (Internet surfers have rights)،هي حملة لمشروع (Verbraucherrechte in der digitalen Welt) "حقوق المستهلك في العالم الرقمي"، تأسست المؤسسة من قبل الجمعية الفيدرالية لحقوق المستهلك وتهدف إلى شرح العالم الرقمي للمستهلكين وتنويرهم حول مخاطر الإنترنت. وتهدف هذه الحملة لرفع مستوى الوعي بممارسات الإنترنت الآمنة: الشبكات الاجتماعية / البلطجة الإلكترونية، محركات البحث، مزود البريد الإلكتروني، ألعاب الكمبيوتر عبر الإنترنت، المزادات على الانترنت، التسوق عبر الانترنت، وكالات التعارف عن طريق الانترنت، قضايا قانونية: حماية البيانات، حماية الشباب، حقوق النشر، قانون العقود[42].

أما حملة (The Watch your web) بالنيابة عن الوزارة الفيدرالية الألمانية لشؤون الأسرة وكبار السن والمرأة والشباب والمفوضية الأوروبية، تهدف الحملة إلى تعزيز وعي الشباب باستخدام الإنترنت بطريقة حرة وآمنة، جميع المواضيع المتعلقة بالشباب، لا سيما المخاطر التي تواجههم في الانضمام إلى الصفحات الرئيسية للشبكة الاجتماعية Facebook StudiVZ) ، SchülerVZ، myspace، lokalisten، wer - kennt - wen، إلخ) وكذا أمن البيانات[43].

2.1.4 المملكة المتحدة:

نجد مؤسسة مراقبة الإنترنت بالمملكة المتحدة (The UK's internet watch foundation) وهي مؤسسة مستقلة ذاتية التنظيم، حيث توفر خطا أخضر وتنبه خدمة للمحتوى غير القانوني المحتمل عبر الإنترنت (بشكل عام، كالصور التي تمثل الاعتداء الجنسي على الأطفال)[44].بينما التحالف الوطني للأمن السيبراني (2001) (National Cyber-Security Alliance) فإن الهدف الأساسي للتحالف هو رفع مستوى الوعي بالتهديدات الإلكترونية التي يتعرض لها الأطفال والآباء والمدرسون وطلاب الجامعات والشركات الصغيرة، يوفر موقع المنظمة للجمهور

E-ISSN : 2571-9742
P- ISSN: 1112-945X

موارد عبر الإنترنت للدفاع عن أنفسهم ضد التهديدات عبر الإنترنت، مثل: التصيد الاحتيالي والبريد العشوائي والاحتيال، فضلاً عن المعلومات التي تساعد الآباء في تعليم أطفالهم حول التهديدات عبر الإنترنت[45].

كما يقدم (OnGuardOnline tips) نصائح من الحكومة الفيدرالية وصناعة التكنولوجيا لمساعدة الجمهور من بينهم الأطفال على حمايتهم من الاحتيال على الإنترنت، وتوفير الموارد لمساعدتهم على تعلم كيفية تأمين أجهزة الكمبيوتر الخاصة بهم وحماية معلوماتهم الشخصية[46].يوفر (Wired Safety) عددًا كبيرًا من الموارد لمستخدمي الإنترنت حول كيفية الحفاظ على أمانهم عبر الإنترنت، يغطي الموقع مجموعة من الموضوعات من الشبكات الاجتماعية إلى البلطجة الإلكترونية وسرقة الهوية، يمكن للأطفال مشاهدة مقطع فيديو أو قراءة المعلومات أو معرفة المزيد من خلال الفصول المجانية التي يقدمها متطوعون مدربون، كما أن هناك أنشطة بحث وتدريب أخرى متوفرة على الإنترنت[47].كما تم إنشاء المبادرة الوطنية لتعليم الأمن السيبراني (National Initiative for Cyber-Security Education NICE) لبناء *"دولة ذكية على الإنترنت"* من حيث التدريب والتوعية من خلال البرامج التعليمية لما بعد التخرج والتطوير المهني لمحترفي الأمن الفيدراليين، وهي تعمل على توعية الأطفال من حيث تعزيز الوعي الوطني بأمن الفضاء الإلكتروني، ودعم برامج التعليم السيبراني الرسمية، من قدرة الوكالات الفيدرالية على جذب وتوظيف واستبقاء موظفي الأمن السيبراني، تكثيف برامج التدريب والتطوير المهني للقوى العاملة الفيدرالية الحالية للأمن السيبراني[48].

أما (GetNetWise) هي خدمة عامة تقدمها شركات صناعة الإنترنت، ومنظمات المصلحة العامة للمساعدة في ضمان حصول مستخدمي الإنترنت ومن بينهم الأطفال على تجارب آمنة وبناءة وتعليمية، يريد تحالف (GetNetWise) أن يكون مستخدمو الإنترنت من خلال *"نقرة واحدة فقط"* يحصلون على الموارد التي يحتاجون إليها لاتخاذ قرارات مستنيرة بشأن استخدامهم وعائلتهم للإنترنت، حيث تعمل هذه الخدمة على توفير دليل السلامة لحماية الأطفال، نصائح حول البريد العشوائي، نصائح الأمان كالتصفح والتسوق ومشاركة التواصل ودروس الفيديو[49].

3.1.4 هولندا:

E-ISSN : 2571-9742
P- ISSN: 1112-945X

تم في سنة 2017 إطلاق مؤسسة (Tegen Internet Misstanden) .T.I.M وهو ما يعني "ضد إساءة استخدام الإنترنت" باللغة الهولندية)، من خلال هذه المؤسسة يزود الوالدين والمهنيين بمعلومات يمكن الوصول إليها، وينشرون رسالة إخبارية عن التحديات الناشئة وعواقبها الخطيرة المحتملة ، ويعملون أيضًا على إنتاج فيلم إعلامي. إنهم يسعون جاهدين لنشر رسالتهم عبر مواقع التواصل الاجتماعي (Facebook و Instagram و Twitter) ووسائل الإعلام التقليدية (التلفزيون والإذاعة والصحف)، تسعى مؤسسة (T.I.M) إلى زيادة الوعي بالتحديات الخطيرة عبر الإنترنت من خلال إقامة حوار مستمر مع الشباب أنفسهم[50].

4.1.4 فرنسا:

يعمل موقع التصفح الذكي (Surf Smart) على تعزيز المصادقة على الإنترنت لمنع محاولات الاحتيال (مثل سرقة البيانات الشخصية بما في ذلك البيانات المصرفية)، حيث يقدم نصائح مقسمة إلى ثلاث فئات رئيسية[51]:

- حماية البيانات الشخصية (التحقق من عنوان URL لمواقع الويب: ، اختر كلمة مرور آمنة، واحتفظ بكل إيصالك الإلكتروني عند شراء شيء ما على الإنترنت، واقرأ شروط الخدمة)

- رسائل البريد الإلكتروني (استخدم فلتر البريد العشوائي، ولا تنقر على الروابط الموجودة في رسالة بريد إلكتروني عندما لا تعرف المرسل، ولا تفتح الملفات المرفقة عندما لا تعرف المرسل، وتجنب إرسال رقم هاتفك، وإنشاء عناوين بريد إلكتروني مختلفة)

- الكمبيوتر الشخصي (قم بتحديث نظامك بانتظام، واحتفظ بتسجيل الدخول وكلمات المرور الخاصة بك في مكان آمن، وقم بتنشيط خيارات الأمان)

كما تعمل الوكالة الوطنية لأمن نظم المعلومات (National Agency for Security of Information Systems) على تقديم مجموعة من الموارد والبرامج التدريبية عبر موقعها ومن هذا التدريب (التحسيس لأمن الإنترنت، حماية الحاسوب، أمن الشبكات اللاسلكية، الإنترنت والأمن، الشهادات الالكترونية)[52].أما بوابة أمان الكمبيوتر (Computer Security Portal) وهي تحت رعاية الوكالة الوطنية لأمن نظام المعلومات (Agence nationale de la Sécurité des Systèmes d'Information) تحتوي هذه البوابة على نصيحة عامة ونصائح محددة حول مجموعة واسعة من موضوعات الأمان لكل من المستخدمين النهائيين وجماهير الأعمال، تم تصميم المعلومات لكل الجمهور من بينهم الأطفال، بالإضافة إلى شرح المصطلحات الأساسية

E-ISSN : 2571-9742
P- ISSN: 1112-945X

مثل "التصيد الاحتيالي (phishing)"، أي كل المسائل المتعلقة بأمن الإنترنت بشكل عام، بما في ذلك: (الإدارة الإلكترونية، المصادقة، الشهادات الالكترونية، إدارة المخاطر، التشفير / الترميز، كلمات المرور، السياسة الأمنية (الإجراءات ، الوثائق)، تأمين شبكتك(Wi-Fi) ، تأمين جهاز الكمبيوتر الخاص بك، توقيع إلكتروني)[53].

نجد أن اللجنة الوطنية للمعلومات و الحرية (National Commission for Computer and Freedom) وهي سلطة إدارية مستقلة تعزز احترام الخصوصية والحرية على الإنترنت ولها اهتمام بموضوعات متعلقة بالاحتيال مثل: بريد مؤذي، التصيد، بيانات شخصية، كلمات المرور، تأمين شبكات محلية (Wi-Fi)، تحتوي المؤسسة على صفحات (Facebook) و (Twitter) و(Daily motion)، يمكن العثور على مقاطع الفيديو التي تشرح مخاطر إعطاء معلومات شخصية على الإنترنت على سبيل المثال على صفحة(Daily motion)[54].أما موقع (Internet Signalement) فهو يوفر خدمة تنبيه للإبلاغ عن الاحتيال عبر الإنترنت، ويغطي: محاولات جنسية تجاه القصر، التهديدات أو العنف أو التحريض على ارتكاب جريمة، الاتجار غير المشروع (المخدرات ، الأسلحة)، بريد مؤذي، التشهير، التزوير، هناك أيضًا أوراق عمل حول كيفية حماية الكمبيوتر، وكيفية التصرف على الإنترنت بشكل عام، وهو تابع لوزارة الداخلية والأقاليم الخارجية والمجتمعات الإقليمية[55].بينما (Signal Spam) فهو موقع للإبلاغ عن البريد المزعج مع بعض المعلومات ذات الصلة[56].

نجد أيضا حملة العائلة على الإنترنت (f@mily en ligne) إذ تم تنفيذ حملة تليفزيونية والموقع الإلكتروني للحملة الإعلانية الرسمية تستمر لأكثر من أسبوعين على محطات التلفزيون الفرنسية الكبرى في ذروة وقت مشاهدة الجمهور، مع 10إعلانات تجارية وتستهدف مختلف الجماهير من بينهم الاطفال، وشعار موقع الويب يرتبط بالمئات أو المنظمات الخاصة ومواقع المجتمع المدني مع الإعلانات التجارية المتاحة على يوتيوب أيضا، والحملة تحت إشراف وزارة الأسرة الفرنسية وجميع مزودي خدمات الإنترنت الفرنسيين والعديد من المنظمات الخاصة والمجتمع المدني، تعمل هذه الحملة على توعية لأطفال من 11- 17سنة، وأولياء أمور الأطفال: حماية البيانات الشخصية والمصرفية، التدوين الآمن، مواقع غير مرغوب فيها، البريد غير المرغوب فيه، حجب المواد غير المرغوب فيها، مراقبة الوالدين في اعتماد ألعاب الإنترنت، رسالة فورية، الشراء عبر الإنترنت[57].

E-ISSN : 2571-9742
P- ISSN: 1112-945X

5.1.4 سويسرا:

مبادرة (Netcity) برعاية المؤسسة السويسرية لحامية الطفل والبراءة وهي عبارة عن حملة تعليمية وتدريبية موجهة نحو قضايا الأمن السيبراني للتلاميذ من عمر 9 إلى 12 عامًا وتتمثل هذه القضايا في (حماية المعلومات الشخصية، نصائح السلامة لاستخدام كاميرا ويب، التحرش، البلطجة، الإغواء الجنسي، المحتوى عبر الإنترنت)، وهي عبارة عن حافلة تجول من مدرسة إلى أخرى في سويسرا وبالقرب منها، بها طاقم متخصص في أمن المعلومات ويتمتعون بخبرة في التدريس ويوفرون منهجًا للأمن السيبراني للأطفال، حيث يلعب الأطفال ألعاب فيديو لتعليمهم حول الأمن السيبراني ويتم منحهم شهادات بعد الانتهاء بنجاح[58].

6.1.4 إيرلندا:

إجعلها آمنة (Make IT secure) هذا ا لمشروع المشترك يوفر موقعًا شاملاً إلى جانب حملة إعلانية تلفزيونية، والهدف منه حماية الاطفال من: التصيد، سرقة الهوية، برامج التجسس، سلامة الطفل على الانترنت.[59]

7.1.4 نيوزيلندا:

(NetSafe Netbasics) هي واحدة من العديد من الحملات التي أنشأتها مجموعة (Netsafe) بهدف تثقيف ودعم مجموعات مختلفة، فيما يتعلق بقضايا السلامة الإلكترونية. تشمل مجموعة (Netsafe) مجموعة من الشركاء الاستراتيجيين منها وزارة التربية والإنترنت ن ز (The Ministry of Education, and InternetNZ)، يمثل مختلف أعضاء مجموعة (Netsafe) وجهات نظر مختلفة من مجتمع الإنترنت عبر نيوزيلندا، من مجالات تشمل: الحكومة، والتعليم، والقانون، والصناعة، والمجتمع، والآباء ومقدمو الرعاية والشباب، تعمل هذه الحملة بالخصوص على حماية العائلات من: التنزيلات الخطرة، جدار الحماية، حماية كلمة المرور، البقاء آمن عبر الإنترنت، التحديث الآمن، النسخ الاحتياطي للبيانات الهامة[60].

بينما نجد هيكتور وورلد(Hector's World Limited) وهي شركة تابعة لـ (.Netsafe) في أعقاب النجاحات السابقة في نيوزيلندا، منذ عام 2008، بدأت في تعزيز الشراكات الدولية، في كل من المملكة المتحدة وأستراليا من خلال هيئة الاتصالات والإعلام الأسترالية (The Australian Communications and Media Authority)، إن القيمة الأساسية لعالم هيكتور هي إحداث تغيير في حياة الأطفال الصغار (الأطفال من 2 إلى 9 سنوات من العمر، وأولياء أمورهم /

E-ISSN : 2571-9742
P- ISSN: 1112-945X

مقدمي الرعاية والمعلمين)من خلال تزويدهم بالمهارات والمعارف بطريقة محفزة فكريا وعاطفيا للتعرف على العالم الرقمي، الرسوم المتحركة ثنائية الأبعاد عالية الجودة والألعاب والموسيقى بما في ذلك: الحلقات والألغاز والألعاب وملفات الموسيقى MP3 وكتب القصص القابلة للتنزيل والأنشطة ذات الصلة، وثائق الدعم المتاحة للآباء والأمهات والمعلمين في شكل خطط الدروس وغيرها[61].

أما حملة (Schools & ECE) فهي تهدف إلى توصيل موارد (Netsafe)المدمجة (بما في ذلك هيكتور وورلد) مباشرة إلى المدارس، على الرغم من أن فريق (Netsafe) سوف يقدم عروضاً للموظفين و/ أو أولياء الأمور بشأن المواد الخاصة بهم عند الطلب، إلا أنهم يفضلون رؤية المدرسين داخل المدرسة يقدمون جميع جوانب تعليم المواطنة الإلكترونية بأنفسهم، وتغطي هذه الحملة مرافق المدارس والتعليم في مرحلة الطفولة المبكرة موضوعات مثل: الهواتف المحمولة، حقوق النشر، مواقع المدارس، المدونات، شبكات التواصل الاجتماعي، البلطجة والمضايقة، بريد مؤذي[62].أما موقع سلامة الطفل على الانترنت (Child Safety Online) والذي يسيره قسم الشؤون الداخلية (Department of Internal Affairs) يقدم معلومات أساسية للغاية لتثقيف أولياء الأمور حول كيفية توفير بيئة إنترنت آمنة لأطفالهم، وهو يتكون من حوار إعلامي حول السلامة الإلكترونية في محاولة لتنبيه الآباء للتهديدات عبر الإنترنت وفوائدها، وعلى الأخص يتم تزويد الآباء بمبادئ توجيهية حول كيفية إسداء المشورة لأطفالهم بشكل صحيح حول السلامة الإلكترونية[63].كما تم تصميم موقع (The Cyber kidz) لمساعدة الآباء والمدرسين على تثقيف الأطفال حول السلامة على الإنترنت، إذ هناك سبعة "نقاط أمان" موضحة من خلال الشخصيات "نجم الويب" و "أصحاب الأزيز" و "مخالب الخطر"[64].

2.4 حكومات الولايات المتحدة الأمريكية وكندا:

1.2.4 الولايات المتحدة الأمريكية:

يقوم المركز الوطني للأطفال المفقودين والمستغلين (The National Center for Missing and Exploited Children NCMEC)، بالشراكة مع مكتب التحقيقات الفيدرالي (FBI)، ومصلحة الهجرة والجمارك (Immigration and Customs Enforcement)، ودائرة فحص البريد الأمريكي(U.S. Postal Inspection Service) ، وجهاز المخابرات الأمريكية (U.S. Secret Service)، ومنظمات التحقيق الجنائي العسكري (Military criminal investigative organizations)،

E-ISSN : 2571-9742
P- ISSN: 1112-945X

ووزارة العدل الأمريكية (U.S. Department of Justice)، وبرنامج فرقة العمل المعنية بجرائم ضد الأطفال (Internet Crimes Against Children Task Force program)، ووكالات إنفاذ القانون المحلي والولائي(state and local law enforcement agencies)، بإدارة (CyberTipline) الذي يتلقى الخيوط والنصائح المتعلقة بجرائم الاستغلال الجنسي للأطفال المشتبه فيها، يمكن للجمهور تقديم نشاط مشبوه أو استغلال مشتبه فيه إلى(CyperTipeline 24/7). تتم مراقبة (TipLine) من قبل المحللين المدربين تدريباً جيداً الذين يوفرون المعلومات لإنفاذ القانون للتحقيق. وفقًا لـ (NCMEC)، تم تقديم أكثر من 1.7 مليون تقرير حول الاستغلال الجنسي للأطفال المشتبه بهم بين عامي 1998 و ديسمبر 2012[65].

قام المركز (NCMEC) بتطوير (NetSmartz)، وهو برنامج ينشأ موارد تعليمية تفاعلية لسلامة الأطفال من سن 5 إلى 17 عامًا، من خلال الأنشطة المناسبة للأعمار والألعاب ومقاطع الفيديو وعروض الأمان، تُعد (NetSmartz) الأطفال ليتصرفوا بمسؤولية عندما يواجهون قضايا مثل البلطجة الإلكترونية، والمحتوى غير المناسب، والاستغلال عبر الإنترنت، والكشف عن الكثير من المعلومات، والرسائل النصية والاحتيال، بالإضافة إلى ذلك، أنشأ المركز (NetSmartz411)، وهي خدمة عبر الإنترنت للإجابة على الأسئلة حول أمان الإنترنت وأجهزة الكمبيوتر والويب، يوفر الموقع مكتبة عبر الإنترنت للآباء والأمهات للعثور على إجابات لأسئلة الأمان الخاصة وهذا بزيارة www.netsmartz411.org.[66] حاليًا، لدى الآباء مجموعة واسعة من قيود الأمان المتوفرة عبر الإنترنت للمساعدة في حماية أطفالهم، مثل (Sheild Genie) وهو عبارة عن برنامج شامل لمراقبة الوالدين، يسمح للآباء بالحد من الوصول إلى المحتوى والألعاب عبر الإنترنت أو إزالته، وحماية الأطفال من جهات اتصال غير مناسبة، ومراقبة وتسجيل جميع أنشطة الكمبيوتر، وتنبيه السلوك الخطير، وتلقي تنبيهات الخطر عن طريق النص أو البريد الإلكتروني و وضع قيود على مشاركة المعلومات الشخصية.[67]

يعتبر مركز السلامة الإلكترونية والتربية (Center for cyber safety and education) منظمة عالمية غير هادفة للربح ولها مقر في الولايات المتحدة ومكاتبها في لندن وهونج كونج وطوكيو، من خلال برنامجها المتمثل في السلامة الإلكترونية والأمن عبر الإنترنت (Safe and Secure Online Program) ، يساعد الأطفال الأعضاء المتطوعون الذين تتراوح أعمارهم بين 11 و 14 عامًا على تعلم كيفية حماية أنفسهم عبر الإنترنت من (الرسائل الجنسية، سيبرانية

E-ISSN : 2571-9742
P- ISSN: 1112-945X

الحيوانات المفترسة، تطبيق وأمن الموقع، حماية المعلومات، برامج التجسس، بريد مؤذي، التسوق عبر الانترنت، التصيد، البرامج الضارة ،كلمات المرور[68]، وبدعم من (Childnet International)[69]، وهي مؤسسة خيرية مقرها المملكة المتحدة تهدف إلى جعل الإنترنت مكانًا آمنًا للأطفال، حيث بدأ تطبيق (Safe and Secure Online) في 2006 لمعالجة الفجوة الأمنية الموجودة في جهود التوعية بسلامة الأطفال[70].

عملت كل من حكومة كندا والو.م.أ بحماية الأطفال من مخاطر البلطجة الإلكترونية من خلال قانون حقوق الإنسان الكندي وقانون الولايات المتحدة للتحرش الجنسي والتمييز، حيث قضت المحكمة العليا في كندا بأن المؤسسات مسؤولة عن توفير بيئات آمنة لموظفيها حتى لو كان التحرش الجنسي من جانب زميل في العمل، والبلطجة الإلكترونية في المدرسة هي تحت مسؤولي المدرسة، حتى ولو حدثت خارج حدودها أو ساعات المدرسة، فالمؤسسة مسؤولة عن تصحيح المشكلة بغض النظر عن مكان حدوث المضايقة بالفعل، كما ينص قانون الولايات المتحدة على توفير الحماية من التحرش الجنسي والتمييز بين الجنسين بموجب البند التاسع من تعديلات التعليم لعام 1972، يتم توفير حماية إضافية لجميع أشكال التمييز بموجب فقرة الحماية المتساوية في التعديل الرابع عشر لدستور الولايات المتحدة، إلى جانب الفيدرالية المحددة للقوانين (مثل المادتين السادسة والسابعة من قانون الحقوق المدنية لعام 1964 وقوانين حقوق الإنسان بالولايات، وتشير إرشادات الباب التاسع إلى أنه تقع على عاتق المدرسة مسؤولية اتخاذ إجراء عندما يعلمون أو يجب أن يكونوا على علم بالتحرش[71].كما يوفر موقع الويب (Cyber Criminals Most Wanted) لمستخدمي الإنترنت عددًا كبيرًا من الموارد الخاصة بسلامة الإنترنت والأخبار من البلدان في جميع أنحاء العالم. بالإضافة إلى ذلك، يقدم الموقع صوراً لمجرمي الإنترنت المطلوبين والمختطفين والمجرمين، في محاولة لزيادة الوعي بجرائم الإنترنت والمجرمين الذين لم يتم القبض عليهم بعد[72]، ويشمل الموقع[73]: (مقالات إخبارية فيما يتعلق بالجريمة السيبرانية (حول العالم)، دليل سلامة الإنترنت، دليل التسوق عبر الإنترنت، الإرهاب الإليكتروني، تزوير، القرصنة، الخدع، سرقة الهوية، بريد مؤذي، برامج التجسس، الفيروسات والعدوى).

2.2.4 كندا:

E-ISSN : 2571-9742
P- ISSN: 1112-945X

نجد المركز الكندي لمكافحة الإحتيال وكبار المنتهكين الذي أنشأ سنة 1993 (PhoneBusters: The Canadian Anti-Fraud Centre) ، وهو مسير بشكل مشترك بين شرطة الخيالة الكندية الملكية وشرطة مقاطعة أونتاريو ومكتب المنافسة، فهو الوكالة المركزية في كندا التي تجمع المعلومات والاستخبارات الجنائية حول الاحتيال في التسويق الشامل (التسويق عبر الهاتف)، ورسائل الاحتيال في الرسوم المسبقة (مثل غرب إفريقيا)، وشكاوى الاحتيال عبر الإنترنت وسرقة الهوية التي تحتوي على محتوى كندي، من المستهلكين أمريكا الشمالية و / أو الضحايا. لا تجري (CAFC) تحقيقات ، ولكنها تقدم مساعدة قيمة لوكالات إنفاذ القانون في جميع أنحاء العالم، يعمل المركز على تثقيف الجمهور حول مخططات احتيالية محددة، وجمع ونشر المعلومات والإحصائيات والوثائق الخاصة بالضحايا لتقديم المساعدة في التحقيقات لإنفاذ القانون[74].

و في عام 1998، أطلق قسم الجريمة التجارية في مونتريال مشروعا متكاملا لمكافحة الإحتيال في التسويق الشامل، مركز العمليات مرتبط باحتيال التسويق عبر الهاتف (Centre of COLT Operations Linked to Telemarketing Fraud)، وهو عبارة عن عملية مشتركة تشمل الشرطة الملكية الكندية، وخدمة شرطة مدينة مونتريال، ومكتب المنافسة، ووكالة خدمات الحدود الكندية، ومكتب التحقيقات الفيدرالي، ووزارة الأمن الداخلي، ودائرة التفتيش لبريد الأمريكي، ولجنة التجارة الفيدرالية الأمريكية، الذي يعمل على مكافحة الاحتيال التسويقي الشامل، حيث يرتكز على تقديم برامج الوقاية والتثقيف، وتنفيذ عمليات الاعتراض وإجراء تحقيقات الاحتيال في التسويق الشامل، ويهدف أيضًا إلى أن يكون سباقا في وضع حد للأنشطة الاحتيالية وزيادة الوعي العام بهذا النوع من الجرائم[75].كما تعد حملة التوعية بالاحتيال على الأهداف التجارية (Fraud Awareness for Commercial Targets FACT) مبادرة توعوية وتثقيفية لمكتب المنافسة (The Competition Bureau) توفر للجهات التجارية والمنظمات غير الهادفة للربح، الحقائق اللازمة لتجنب الوقوع ضحية للاحتيال ، والتي تكلفهم ملايين الدولارات سنويًا[76].

أما منتدى منع الاحتيال عبارة عن مجموعة معنية من شركات القطاع الخاص، ومجموعات المستهلكين والمتطوعين، والوكالات الحكومية ومنظمات إنفاذ القانون، الملتزمة بمكافحة الاحتيال الذي يستهدف المستهلكين والشركات، من خلال شركائه، يعمل المنتدى

E-ISSN : 2571-9742
P- ISSN: 1112-945X

الذي يرأسه مكتب المنافسة، على منع الكنديين من أن يصبحوا ضحايا للاحتيال عن طريق تثقيفهم حول كيفية التعرف عليه، ومنع هذه المشكلة وضمان الثقة في السوق، ينظم المنتدى حملة توعية لمدة شهر كامل والمتمثل في شهر مارس لتحسين وعي المستهلكين وفهمهم لمخاطر الاحتيال، حيث يتم تنظيم الأحداث من قبل أعضاء المنتدى الذي يتكون من أكثر من 100 منظمة خاصة وعامة، وتنطلق حملة إعلانات الخدمة العامة في الصحف اليومية باللغتين الفرنسية والإنجليزية وعلى محطات الإذاعة والتلفزيون في جميع أنحاء البلاد مع إعلانات على التلفزيون والإذاعة والمطبوعات [77].

3.4 حكومات آسيا:

1.3.4 هونغ كونغ:

موقع (Information Security is Everybody's Business- INFOSEC) هو من أجل الرد على إساءة استخدام الإنترنت من قبل المجرمين، تتمثل مهمة أمن المعلومات (InfoSec) في العمل كبوابة واحدة لعامة الناس(الأطفال والشباب، الآباء والأمهات والمعلمين، محترفي تكنولوجيا المعلومات، الشركات الصغيرة والمتوسطة) للوصول الفعال إلى المعلومات والموارد المتعلقة بأمن المعلومات، وكذلك التدابير وأفضل الممارسات لمنع الجرائم السيبرانية، من خلال: الأخبار والأحداث، الترويج والتعليم العام، أمن المعلومات، الفيروسات والرموز الخبيثة، حماية نفسك (الاستخدام المقبول للإنترنت، والحفاظ على الوعي الذاتي بأمن المعلومات، والتعامل مع حسابات المستخدمين وكلمات المرور، والتعامل مع معلوماتك الشخصية، وحماية الأجهزة المحمولة، واستخدام المراسلة الفورية بأمان، واستخدام البريد الإلكتروني بحكمة، واستخدام البرامج، واستخدام أجهزة الكمبيوتر العامة بعناية وأمن الشبكات الاجتماعية عبر الإنترنت، وتصفح الإنترنت الآمن والتسوق الإلكتروني، والتعامل مع الحوادث الأمنية للأفراد، والحماية من رسائل البريد الإلكتروني العشوائي، والحماية من هجمات الخداع، والحماية من الرموز الضارة، والحماية من برامج التجسس والبرامج الإعلانية، والمدونة بأمان، وتأمين شبكتك اللاسلكية)، قم بحماية جهاز الكمبيوتر الخاص بك،حماية عملك، الجرائم المتعلقة بالحاسوب، مكافحة الخداع[78].

أما المبادرة الحكومية هونغ كونغ يوم نظيف للكمبيوتر(Hong Kong Clean PC Day – OGCIO, HK CERT and Hong Kong Police) هي جهد تثقيفي لعامة الناس حول الوعي بأمن

E-ISSN : 2571-9742
P- ISSN: 1112-945X

المعلومات، لها حملة ترويجية تتبع موضوعًا مختلفًا كل سنة منها مثلا: أمان المعاملات عبر الإنترنت (2009)، أمن المعلومات للشباب (2008)، إدارة الأمن للشركات (2007)، السلامة الحاسوبية الشخصية الأساسية للجمهور (2006)[79].

2.3.4 كوريا:

وكالة كوريا لأمن المعلومات (KISA Korea Information Security Agency) هي عبارة عن مزيج من وكالة أمن المعلومات الكورية، والوكالة الوطنية لتطوير الإنترنت ووكالة التعاون الدولية لتكنولوجيا المعلومات الكورية، وهذا من أجل حماية المجتمع بشكل عام والأطفال من القرصنة و سرقة الهوية[80].

3.3.4 سنغافورة:

منتزه الأمن الافتراضي عبر الإنترنت (Virtual Cyber-Security Park) في محاولة لتعليم أطفال المدارس على الأمن السيبراني الجيد، حيث فتحت سنغافورة "هذا المنتزه، وتم الإعلان عنه في مارس 2010 كجزء من (Infocomm Security Masterplan 2) إذ أتاح للتلاميذ الذين يدرسون بالمدرسة الابتدائية في سنغافورة الفرصة للتجول في (Virtual Cyber-Security Park) لتعلم الأمن السيبراني الجيد بطريقة جذابة وممتعة[81].أما موقع ذات مرة على الفضاء الإلكتروني (Once Upon a Cyberspace)والذي عملت هيئة تطوير الوسائط (Singapore Media Development Authority) وهي هيئة تنظيمية سنغافورية، على تأدية دورًا نشطًا في الترويج لـ "Cyber Wellness"، حيث يعد تشغيل سلسلة الرسوم المتحركة "ذات مرة على الفضاء الإلكتروني" واحدة من الطرق المختلفة التي يحاولون من خلالها الوصول إلى المجتمع، والهدف منه حماية الأطفال من سن 10-14 سنة من مخاطر مشاركة المعلومات الشخصية عبر الإنترنت، لعبة الإدمان، فيروسات الإنترنت، البلطجة السيبرانية، انتهاك الخصوصية[82].

4.3.4 اليابان:

موقع تأمين اليابان (Secure Japan 2009)، وهو تابع للمركز القومي لأمن المعلومات (National Information Security Centre) و الهدف الرئيسي لهذا الموقع الحكومي هو أنه يجب "افتراض" وقوع الحوادث ، أي أن خروقات الأمن أمر لا مفر منه، وبالتالي يجب التركيز أكثر على الاستجابة لهذه الأزمات وكذلك على التدابير الوقائية. إنه يحتوي على مواد للعديد من الجماهير بما في ذلك الأطفال، وهو يغطي الموضوعات الآتية: تعزيز الوعي بالمجتمع عبر

E-ISSN : 2571-9742
P- ISSN: 1112-945X

الإنترنت، تشفير آمن، الاستفادة من منتجات تكنولوجيا المعلومات آمنة وموثوقة، حوكمة أمن المعلومات، تدابير مكافحة البريد المزعج، المواقع الخبيثة، تجنب البرامج الضارة[83].

4.4 الجمعيات والمنظمات العالمية:

إن مجموعة عمل مكافحة التصيد (APWG, The Anti-Phishing Working Group) هي جمعية عالمية تركز على القضاء على السرقة و الاحتيال والهوية التي تنجم عن الخداع والتزوير عبر البريد الإلكتروني بجميع أنواعه[84].أما موقع (Security Cartoon)فهو نتاج كل الدكاترة (Sukamol Srikwanو Markus Jakobsson) اللذان قاما بتطوير موقع (Security Cartoon) في عام 2006، كنهج لتحسين الوعي الأمني والتفاهم بين مستخدمي الإنترنت العاديين، وهذا باستخدام الرسوم لتدريس أمن الإنترنت، يقدم موقع (Security Cartoon) نظرة عامة عن التهديدات السيبرانية مثل (الخداع، البرامج الضارة، التصيد، حماية كلمات المرور، السياسة والخصوصية) وهذا باستخدام الرسوم، إنه يقدم طريقة مبتكرة لتثقيف الجمهور حول السلامة الشخصية على الإنترنت، حيث يتم تلخيص شدة المخاطر التي ينطوي عليها كل موضوع في شريط هزلي قصير في محاولة لجذب انتباه المستخدمين[85].

5. خاتمة:

يعكس الالتزام القوي بحماية الأطفال من العنف بشكل واضح في أهداف التنمية المستدامة والعمل الأخير للحكومات والشراكات في جميع أنحاء العالم، بما في ذلك الشراكة العالمية لإنهاء العنف ضد الأطفال، إذ نحن بحاجة إلى حماية أطفالنا حتى يتمكنوا من حماية أنفسهم وتزويدهم بالمهارات والمعرفة حتى يتمكنوا من التنقل في حياتهم الإلكترونية وحياة الواقع بأمان وحكمة.إن التجارب الدولية في مجال حماية الاطفال من مخاطر المعلوماتية هو تفكير تخطيطي وله أبعاد مستقبلية من أجل تكوين مواطن صالح يخدم البلد والمجتمع ككل، ويزيد من صيغة التطور للبنية التحتية ويفتح أفاق للتفكير الإيجابي من أجل دعم الوطن من جميع النواحي الاقتصادية والاجتماعية والثقافية والسياسية وغير ذلك من الطاقات المستقبلية السوية. تكوين أطفال أذكياء يتطلب التضحيات وتكاثف الجهود لكل القطاعات داخل الحكومة الواحدة، فالكل معني بحماية البراءة من مخاطر المعلوماتية التي لها أثار مستقبلية سلبية إن لم تتم التوعية والردع القانوني والتكنولوجي والإجتماعي لمثل هكذا تصرفات مشينة، فأطفال اليوم هم رجال ونساء الغد، لدى علينا الآن التفكير مليا في بذل

E-ISSN : 2571-9742
P- ISSN: 1112-945X

الجهود أكثر من أجل نشء سوي ويتميز بصفات تجعلنا نعتمد عليه في تسير البنية التحتية المجتمعية المستقبلية.

تستكشف اليونيسف على نحو متزايد كيف يمكن استخدام تكنولوجيا المعلومات والاتصالات في برامج حماية الطفل، مثل تيسير تسجيل المواليد، والتتبع السريع للأسرة وإدارة الحالات، وتشارك اليونيسف أيضاً في الدعوة إلى تجريم مواد الاعتداء الجنسي على الأطفال والاستمالة عبر الإنترنت للأطفال؛ تعزيز القدرات المؤسسية لتنفيذ التشريعات والسياسات المتعلقة بالتحقيق والمقاضاة في القضايا التي تنطوي على اعتداء جنسي / استغلال جنسي عبر الإنترنت؛ دعم إنشاء خدمات شاملة للأطفال الذين يتعرضون للإيذاء / الاستغلال من خلال الإنترنت والهواتف المحمولة؛ إذكاء الوعي وبناء قدرات الأطفال والمعلمين ومقدمي الرعاية بشأن مخاطر تكنولوجيا المعلومات والاتصالات والتدابير الوقائية ودعم مشاريع البحوث لتعزيز فهم استخدام الأطفال لتكنولوجيا المعلومات والاتصالات والاستجابات المناسبة للعنف والاستغلال وسوء المعاملة التي تيسرها تكنولوجيا المعلومات والاتصالات[86].

الهوامش:

[1] - Unicef for every child. Annual Report 2018. New York : United Nations Children's Fund, 2019, P27 https://www.unicef.org/media/55486/file/UNICEF-annual-report-2018%20revised%201.pdf

[2]- عبد الرحمن بدوي. مناهج البحث العلمي. ط3. الكويت: وكالة المطبوعات. 1977.[على الخط] file:///C:/Users/annotec124/Downloads/elebda3.net-wq-3182.pdf

[3] - Unicef for every child. Child protection and Information and Communication Technologies (ICTs). Updated: 3 January 2018. https://www.unicef.org/protection/57929_79672.html

[4] - secure kids. Do we protect our children from the internet dangers? 22/09/2017. https://securekids.es/en/internet-danger/

[5] - Unicef for every child. Child protection and Information and Communication Technologies (ICTs). Updated: 3 January 2018. Op. Cit.

[6] - Martina J. Zucule de Barros and Horst Lazarek. A Cyber Safety Model for Schools in Mozambique. In Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018), pages 251-258. DOI: 10.5220/0006573802510258

[7] - World Health Organization. Safety and security on the Internet Challenges and advances in Member States : Based on the findings of the second global survey on eHealth : Global Observatory for eHealth series - Volume 4. Switzerland : WHO

E-ISSN : 2571-9742
P- ISSN: 1112-945X

Library Cataloguing-in-Publication Data, 2011. P16
https://www.who.int/goe/publications/goe_security_web.pdf

[8] - secure kids. Op. Cit.

[9] - Stuart Dredge.
How do I keep my children safe online? What the security experts tell their kids. **Mon 11 Aug 2014** https://www.theguardian.com/technology/2014/aug/11/how-to-keep-kids-safe-online-children-advice

[10] - UNICEF. #ENDviolence online.
https://www.unicef.org/endviolence/endviolenceonline/

[11] - Kidpower Teenpower Fullpower International. **How To Keep Kids Safe OnlineTen Kidpower Recommendations For Parents And Guardians.** March 8, 2012, Last Updated: August 29, 2017
https://www.kidpower.org/library/article/internet-safety/

[12] - Ann Brenoff. **How To Protect Your Child Online, According To A Cybersecurity Expert.** In : *life*, 03/09/2018.
https://www.huffpost.com/entry/theresa-payton-keep-kids-safe-online_n_5a944d02e4b02cb368c46c87

[13] - UNICEF. #ENDviolence online. Op. Cit

[14] - Social, Health and Family Affairs Committee ; Nicolas About. Abuse and neglect of children. Doc. 8041. 17 March 1998.
http://www.assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewHTML.asp?FileID=8367&lang=en

[15] - Ibid.

[16] - Carrie Dunn. Is technology helping families communicate or holding them back? . Tue 6 May 2014. https://www.theguardian.com/society/2014/may/06/technology-helping-families-communicate-or-holding-back

[17] - Ibid.

[18] - Erica Dawn Shifflet. INFORMATION TECHNOLOGY AND THE NET GENERATION: THE IMPACT OF TECHNOLOGY ON ADOLESCENT COMMUNICATION AND INTERACTION. Social Work- Doctor of Philosophy. Michigan State University. 2013. P27-28
https://pdfs.semanticscholar.org/22ef/49f4b93318959bb22b0a6018e316d59755b2.pdf

[19] - Kidpower Teenpower Fullpower International. **Op. Cit.**

[20] - Erica Dawn Shifflet. Op. Cit. P31-32.

[21] - Unicef for every child. Child protection and Information and Communication Technologies (ICTs). Updated: 3 January 2018. Op. Cit.

[22] - Shaheen Shariff, Dianne L. Hoff. **Cyber bullying: Clarifying Legal Boundaries for School Supervision in Cyberspace**. In : *International Journal of*

E-ISSN : 2571-9742
P- ISSN: 1112-945X

Cyber Criminology, Jan. 2007, vol 01, issue 1, pp76-118 DOI: 10.5281/zenodo.18279

23 - Unicef for every child. Child protection and Information and Communication Technologies (ICTs). Updated: 3 January 2018. Op. Cit.

24 ˉ Shaheen Shariff, Dianne L. Hoff. **Op. Cit.**

25 - Livingstone, Sonia. Regulating the internet in the interests of children: emerging European and international approaches. In: Mansell, Robin and Raboy, Marc, (eds.) The Handbook of Global Media and Communication Policy. Wiley-Blackwell, Oxford, UK, 2011, pp. 505-524. ISBN 9781405198714

26 - Ibid.

27 - Ibid.

28 - Chris Connolly, Alana Maurushat ,David Vaile (et al.); Additional research: Stephanie Cuevasn, Melissa Wong. An Overview of International Cyber-Security Awareness Raising and Educational Initiatives. Australian: Galexia, 2011, p 26.

29 - A European Strategy to deliver a Better Internet for our Children https://ec.europa.eu/digital-single-market/en/european-strategy-deliver-better-internet-our-children

30 - Ibid.

31 - Livingstone, Sonia. Op. Cit.

32 - Connecting Europe Facility in Telecom https://ec.europa.eu/digital-single-market/en/connecting-europe-facility

33 - Horizon 2020 https://ec.europa.eu/programmes/horizon2020/

34 - Livingstone, Sonia. Op. Cit.

35 - Ibid.

36 - Better internt for kids. **Dangerous online challenges.** 28/06/2019 https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=4696122

37 - Ibid.

38 - Livingstone, Sonia. Op. Cit. pp. 505-524

39 - Bundesamt für Sicherheit in der Informationstechnik https://www.bsi.bund.de/DE/DasBSI/dasbsi_node.html;jsessionid=AE34D084D27C1DDB8F36D06EE1564756.1_cid341

40 - www.klicksafe.de https://www.klicksafe.de/

41 - polizei – beratung.de https://www.polizei-beratung.de/typo3conf/ext/mq_layout_propk/Resources/Public/Images/main/layout/logo.png

42 - surfer-haben-rechte https://www.surfer-haben-rechte.de/

43 - Watch your web http://www.watchyourweb.de/

44 - Livingstone, Sonia. Op. Cit.

E-ISSN : 2571-9742
P- ISSN: 1112-945X

45 - stay safe online by National Cyber-Security Alliance https://staysafeonline.org/
[46] - Federal trade commission : consomer information https://www.consumer.ftc.gov/features/feature-0038-onguardonline
47 - wired safety https://www.wiredsafety.com/
48 - NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE) https://www.nist.gov/itl/applied-cybersecurity/nice
49 - Get Net Wise http://www.getnetwise.org/index.php/about/
50 - Better internt for kids. **Op. Cit.**
51 - Surfez Intelligent – Les Indispensables http://surfez-intelligent.dgmic.culture.gouv.fr/spip.php?rubrique8
[52] - Agence nationale de la Sécurité des Systèmes d'Information http://www.ssi.gouv.fr/
[53] - Ibid.
[54] - Commission Nationale Informatique et Libertés https://www.cnil.fr/
[55] - internet signalement. Gov.fr : portail official de signalement des contenus illicites de l'internet https://www.internet-signalement.gouv.fr/PortailWeb/Accueil!input.action
[56] - Signal Spam https://www.signal-spam.fr/
[57] - ENISA : the European Union Agency for Cybersecurity https://www.enisa.europa.eu/activities/awareness-raising/deliverables/2007/loc=gov/en
[58] - Netcity http://www.netcity.org/
[59] -MAKE IT SECURE www.makeitsecure.org
[60] - Net safe online safety for new zealand https://www.netsafe.org.nz/
[61] - Hector's world http://www.hectorsworld.com/
[62] - Net safe online safety for new zealand. Op. Cit
[63] - Department of Internal Affairs https://www.dia.govt.nz/
[64] - Ibid.
[65] - shared hope international, SHI STAFF. **5 Scary Statistics About Internet Safety**. AUGUST 7, 2013 https://sharedhope.org/2013/08/07/5-scary-statistics-about-children-on-the-internet/
[66] - Ibid.
[67] - Ibid.
[68] - Center for cyber safety and education. https://www.iamcybersafe.org/s/
[69] - https://www.childnet.com/
[70] - center for cyber safety and education. Op. Cit.
[71] - Shaheen Shariff, Dianne L. Hoff. Op. Cit.
[72] - Cyber Criminals Most Wanted http://www.ccmostwanted.com/
[73] - Chris Connolly, Alana Maurushat ,David Vaile (et al.). Op. Cit. p 24.

E-ISSN : 2571-9742
P- ISSN: 1112-945X

[74] - PhoneBusters: The Canadian Anti-Fraud Centre, and SeniorBusters http://www.antifraudcentre-centreantifraude.ca/english/index.html

[75] - Royal Canadian Mounted Police http://www.rcmp-grc.gc.ca/en/qc/home

[76] - FACT: Fraud awareness for commercial targets https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/02600.html

[77] - Fraud prevention forum partners http://www.ic.gc.ca/eic/site/cb-bc.nsf/eng/01842.html

[78] - INFO SEC http://www.infosec.gov.hk/english/sme/sme.html

[79] - INFO SEC http://www.infosec.gov.hk/english/promotion/campaign.html

[80] - Korea Internet & Security Agency (KISA) https://www.kisa.or.kr/eng/aboutkisa/presidentGreetings.jsp

[81] - The asian parent Singapore https://sg.theasianparent.com/virtual-cyber-security-park-singapore

[82] - Chris Connolly, Alana Maurushat ,David Vaile (et al.). Op. Cit. p 70.

[83] - National center of Incident readiness and Strategy for Cybersecurity https://www.nisc.go.jp/eng/

[84] - APWG https://apwg.org/

[85] - SecurityCartoon.com http://www.securitycartoon.com/about.php

[86] - Unicef for every child. Child protection and Information and Communication Technologies (ICTs). Updated: 3 January 2018. Op. Cit.