نشریهٔ ایرانی مطالعات شهروندی
سال اول، شمارهٔ دو/ زمستان ۱۴۰۲/ صفحه ۵۳ـ۸۴
نوع مقاله: علمی‌پژوهشی
تاریخ دریافت: ۱۴۰۲/۹/۱۲ تاریخ پذیرش: ۱۴۰۲/۱۲/۲۲

آموزش شهروندی نوین و امنیت (کارکردها و ضرورت‌ها)

الهام ایران‌نژاد،[۱*] علی مهداد،[۲] محسن گل‌پرور[۳]

چکیده

امروزه بیش از نیمی از جمعیت کرهٔ زمین در شهرها زندگی می‌کنند. ابعاد مختلف مسائل و بحران‌های شهری، پیوند میان شهروندی و امنیت را افزایش داده است. بر این اساس، امنیت از شکل سنتی جانی، مالی، تجاری، حساب‌های بانکی و معاملات خارج شده و به ابعاد تازهٔ توسعهٔ پایدار، محیط‌زیستی، رسانه‌ای و دیجیتالی معطوف گردیده تاحدی‌که برای ابعاد نوین آن، پلیس تخصصی فتا (فضای تولید و تبادل اطلاعات) با هدف تأمین امنیت فضای مجازی، حفظ امنیت و آزادی‌های مشروع شهروندان و حفظ زیرساخت‌های کشور در برابر حمله‌ها و جرائم سایبری تشکیل شده است تا پیگیر برقراری امنیت در این حوزه باشد. این پژوهش به‌صورت مروری و بر پایهٔ پیشینهٔ موجود، ارتباط بین امنیت و رفتارهای شهروندی را بررسی کرده که به‌صورت نمونه‌گیری از متون علمی موجود در این زمینه و بر مبنای رسیدن به اشباع اطلاعاتی است. بررسی ۵۲ مقاله، کتاب و کتابچه، نشان داد که شناخت حق و مسئولیت‌ها که در قالب آموزش‌های شهروندی ارائه می‌شود، راهی مؤثر برای پیشگیری از جرائم و آگاهی‌رسانی به شهروندان برای حفاظت از خود است. همچنین آموزش شهروندی می‌آموزد که در برخورد با مواردی که امنیت آن‌ها را به خطر می‌اندازد، چگونه رفتار کنند و به کجا مراجعه کنند. آگاهی شهروندان و گزارش زودهنگام موارد مشکوک و جرائم سایبری به پلیس فتا، در شناسایی و پیگیری جرائم کمک کرده و احتمال درگیری ناخواستهٔ افراد جامعه در چنین جرائمی را کاهش می‌دهد و پیشگیری با قدرت و بهتر انجام می‌شود.

کلیدواژه‌ها: شهروندی، امنیت، فضای مجازی، پلیس فتا.

---

۱. دانشجوی دکتری روان‌شناسی تربیتی، واحد اصفهان (خوراسگان)، دانشگاه آزاد اسلامی، اصفهان، ایران، نویسندهٔ مسئول، elhamirannegad@yahoo.com
۲. دانشیار، گروه روان‌شناسی، واحد اصفهان (خوراسگان)، دانشگاه آزاد اسلامی، اصفهان، ایران، alimahdad.am@gmail.com
۳. استاد، گروه روان‌شناسی، واحد اصفهان (خوراسگان)، دانشگاه آزاد اسلامی، اصفهان، ایران، drmgolparvar@hotmail.com

Doi: 10.22052/IJCS.2024.253891.1023

۱. مقدمه

شهروندی از سازه‌های مهم سیستم‌های سیاسی و اجتماعی مدرن است (قیان،[1] ۲۰۲۰). در فرهنگ لغت انگلیسی، واژهٔ شهروندی به‌معنای القای رفتار اجتماعی مطلوب، با توجه به ارزش‌های جامعه است تا شهروندانِ خوبی شکل بگیرند (القتاونه[2] و همکاران، ۲۰۱۹). امروزه با گسترش شهرنشینی، به‌گونه‌ای که بیش از نیمی از جمعیت کرهٔ زمین در شهرها زندگی می‌کنند و با توجه به اینکه شهرها دارای مسائل و بحران‌هایی در ابعاد مختلف‌اند که امنیت را تحت‌تأثیر می‌گذارند، پیوند میان شهروندی و امنیت بسیار زیاد شده است. تعریف امنیت عبارت است از: حفاظت از یک فرد، ساختمان و سازمان یا کشور در برابر تهدیدها، رهایی از خطر و تهدیدِ تغییر به‌سوی بدتر شدن، حفاظت از اطلاعات در برابر سرقت یا استفادهٔ نادرست یا غیرقانونی، احساس امنیت از شغل، پول و... و از دست نرفتن آن‌ها، و مانند آن (کمبریج، ۲۰۲۲). امنیت در گذشته بیشتر بر جنبه‌های فیزیکی و نظامی تأکید داشت که بخش ابتدایی امنیت محسوب می‌شود (هادی‌سیفی و همکاران، ۱۳۹۸)؛ اما در دیدگاه نوین، امنیت مقوله‌ای وسیع، معین، غیرانحصاری، عقلانی، هدفمند و پایدار است و هویت، احساسات و عواطف فردی و گروهی، عقاید، تمایلات، موقعیت‌های شغلی و اقتصادی، باورهای فرهنگی و ساختارهای رسمی و حتی وسایل دستیابی به رفاه و آسایش زندگی اجتماعی را دربردارد (کن،[3] ۲۰۲۴؛ ماهر،[4] ۲۰۲۴؛ متقی و داودی، ۱۴۰۰).

فناوری‌های رسانه‌ای نوین، توانایی تولید، اشتراک‌گذاری و نقد محتوای رسانه‌ای به افراد داده است که این فعالیت‌ها نیاز به سواد رسانه‌ای دارد. بنابراین، توانایی درک و کاربرد درست رسانه‌های نوین، بخشی ضروری از زندگی مدرن شده است (آدتورو و اکیکه،[5] ۲۰۲۲). رسانه‌های همگانی، امروزه نقش مهمی در اجتماعی شدن دارند و بیشتر مردم از رسانه‌های گروهی، اخبار و اطلاعات را دریافت می‌کنند. رسانه‌ها به این دلیل که

1. Qian
2. Al-Qatawneh
3. Cann
4. Maher
5. Adetoro & Okike

بر میزان و روشنی اطلاعات منتشرشده اثر دارند، می‌توانند بر احساس امنیت و پایداری در جامعه اثر داشته باشند (عشایری و همکاران، ۱۴۰۰). رسانه‌های اجتماعی اثر زیادی بر شکل‌گیری دانش گروهی دارند. ادراکی که به دیگران منتقل می‌کنند، تابعی از شیوهٔ القا، سوگیری‌ها، الگوهای ذهنی و رفتاری و عوامل اجتماعی است. محتوا و ساختار رسانه ازنظر روان‌شناختی توجه را به خود جلب می‌کنند (فیروزی و همکاران، ۱۴۰۰) و تصویری که در ذهن مردم می‌سازند، همیشه با واقعیت همخوان نیست و چگونگی بازنمایی رویدادها، می‌تواند باعث افزایش احساس امنیت و آسودگی یا ایجاد ترس و حس قربانی بودن در شهروندان شود که ممکن است باعث ترس و احساس ناامنی گردد (عشایری و همکاران، ۱۴۰۰).

اینترنت به‌عنوان بستری برای رسانه‌های نوین، می‌تواند به ارضای نیازهای جدید و یا ارضای نیازهای قبلی با روش‌های جدید بپردازد. این فناوری برای کاربران خود، روش‌های ارتباطی جدید، منعطف و کم‌هزینه‌ای را فراهم کرده است. حضور در رسانه‌های مجازی به کاربران فرصت‌های بی‌شماری می‌دهد و به هر اندازه که این فرصت‌ها و خشنودی‌های ناشی از استفاده از اینترنت افزایش یابد، کاربران بیشتر به‌سمت این پدیدهٔ نوین سوق خواهند یافت (سیف‌درخشنده و همکاران، ۱۴۰۰). ازسوی دیگر، شهروندی رسانه‌ای دربرگیرندهٔ نگرانی‌هایی همچون انتشار اطلاعات نادرست، ناراحتی از پست‌های نامناسب، هک کردن، جریحه‌دار شدن احساسات، نبودن حریم خصوصی، وجود عکس‌های نامناسب و قلدری است که همهٔ این عوامل باعث ناامنی روانی می‌شود و اگر فرد نداند چگونه اقدام کند تا از خود محافظت کند و از تعاملات ناخواسته جلوگیری کند، همیشه دچار نگرانی و اضطراب خواهد بود (گرامون،[1] ۲۰۲۰). در رسانه‌های اجتماعی، کاربر پروفایل خود را دست‌کاری می‌کند تا یک هویت آنلاین بسازد. استفاده از رسانه‌های اجتماعی علاوه‌بر کمک به ایجاد هویت آنلاین، در برخی از

1. Grammon

زمینه‌های عاطفی، شناختی، اجتماعی و عادتی زندگی کاربران، وارد شده و منافع و مضراتی به دنبال داشته است (کریستینسن[1] و همکاران، ۲۰۱۸).

در این مقاله به مشکلات مدرن امنیتی ایجادشده برای شهروندان اشاره می‌شود که می‌توان به کمک آموزش‌های شهروندی آن‌ها را تا حد زیادی کنترل کرد و امنیت اجتماعی شهروندان را افزایش داد.

۲. ابعاد جامع شهروندی نوین

امنیت از نگاه سنتی بر پایهٔ دفاع از آب و خاک و تمامیت ارضی، مشارکت در سازندگی و رعایت قوانین کشور برای ایجاد امنیت عمومی برای همهٔ شهروندان با ابعاد سنتی شهروندی، سیاسی، مدنی و اجتماعی پیوند دارد (بیسوس و مورای،[2] ۲۰۲۴). از دیدگاه روان‌شناسی اجتماعی، شهروندی که به حقوق خود و جامعه آگاه باشد، با درک خود به‌عنوان عضوی از جامعه و پذیرش تکالیف خود در قبال آن جامعه، خود را مکلف به انجام تعهدات می‌نماید. بدین‌گونه مفهوم مشارکت و شهروندی به هم پیوند می‌خورد، به‌شکلی که مشارکت، پیش‌نیاز و جزئی جدانشدنی از شهروندی می‌شود (گل‌بهاری و رجبلو، ۱۳۹۹). شهروندی، در قرن ۲۱، نه‌تنها به آگاهی شهروندان از حقوق خود، بلکه به خواست آن‌ها برای فعالیت مستقل اشاره دارد، به‌گونه‌ای که تصمیم و رفتار آن‌ها، بازتاب ملاحظات اخلاقی، عدالت اجتماعی و کرامت انسانی باشد (القتاونه و همکاران، ۲۰۱۹؛ رجکینینگسیه،[3] ۲۰۱۵).

شهروندی سیاسی به مشارکت فعال در مسائل سیاسی همچون شرکت در انتخابات و کمپین‌های انتخاباتی (آندرولی و بریس،[4] ۲۰۲۲)، تمایل به جانب‌داری از گروه خاص، متقاعد کردن دیگران به رأی دادن یا طرف‌داری از سیاست خاص گفته می‌شود (ستیدپرن،[5] ۲۰۲۲). شهروندی مدنی شامل احترام کامل به حقوق بشر، مانند برابری

1. Christensen
2. Biswas & Murai
3. Rejekiningsih
4. Andreouli & Brice
5. Satidporn

به‌عنوان مبنایی برای دموکراسی، ارج نهادن و درک تفاوت‌های بین نظام‌های ارزشی گروه‌های مذهبی یا قومی مختلف، نشان دادن احساس تعلق به محل، کشور و تمایل به مشارکت در همهٔ سطوح جامعه است (هوسکینز،[1] ۲۰۰۸).

در نگاه امروزی، شهروندی به حوزه‌های اجتماعی خارج از قلمرو حکومت هم گسترش یافته که به کمک آن، ارزش‌ها و معانی فرهنگی می‌توانند در مقطعی مبادله و نهادینه شوند. شهروندی اجتماعی، در مورد انسجام اجتماعی، همزیستی افراد و ایجاد هویت‌های اجتماعی (نیوولینک و اوستدام،[2] ۲۰۲۱)، درگیر شدن در رفتارهای مثبت نسبت به دیگر اعضای جامعه است (بروم،[3] ۲۰۲۰). همچنین ابعاد نوین معطوف به کلیت محیط و جامعهٔ انسانی، ازجمله شهروندی زیست‌محیطی است که شامل مشارکت فعال فردی و گروهی شهروندان، در حوزه‌های خصوصی و عمومی، برای حل مشکلات زیست‌محیطی جاری و پیشگیری از ایجاد موارد تازه به‌همراه ایجاد یک رابطهٔ سالم با طبیعت است (تلسین[4] و همکاران، ۲۰۲۱).

از نگرانی‌های دیگر، مسئلهٔ پایداری است که به برآورده کردن نیازهای حاضر، بدون به خطر انداختن توانایی نسل‌های آینده در برآوردن نیازهای خود توجه دارد (کاو،[5] ۲۰۱۸). هیچ اقدام و سیاست پایداری بدون همکاری مؤثر شهروندان و رعایت حقوق و انجام وظایف ازسوی آن‌ها، موفق نخواهد شد. شهروندان با انتخاب سبک زندگی به‌شیوه‌ای پایدار می‌توانند به عدالت درون‌نسلی و بین‌نسلی کمک کنند (هاجی‌چامبیس و هاجی‌چامبی،[6] ۲۰۲۰). همچنین گسترش ظرفیت‌های استفاده از فضای مجازی و رسانه‌ها، ابعاد تازه‌ای موسوم به شهروندی رسانه‌ای و دیجیتالی را در حوزهٔ شهروندی مدرن به وجود آورده است. این حوزهٔ شهروندی با امنیت غذایی، امنیت آب و پایداری و امنیت در محیط زیست شهروندی و اکولوژیک، تأمین غذا و مسائل این‌چنینی در ارتباط است که در دورهٔ

1. Hoskin
2. Nieuwelink & Oostdam
3. Broom
4. Telešienė
5. Cao
6. Hadjichambis & Hadjichambi

میانی توجه به شهروندی به ابعاد سنتی شهروندی افزوده شد (ژو[1] و همکاران، ۲۰۲۴)

فناوری‌های رسانه‌ای نوین، توانایی تولید، اشتراک‌گذاری و نقد محتوای رسانه‌ای به افراد داده است که این فعالیت‌ها نیاز به سواد رسانه‌ای دارد. بنابراین، توانایی درک و کاربرد درست رسانه‌های نوین، بخشی ضروری از زندگی مدرن شده است (آدتورو و اکیکه، ۲۰۲۲). همچنین شکل، محتوا و کیفیت تعاملات انسانی و در پی آن کنش‌های مدنی و سیاسی دستخوش دگرگونی شده است (احمدی و مرادی، ۱۳۹۷). بخش بزرگی از رسانه‌های امروز به‌صورت مجازی و دیجیتال‌اند که باعث گره خوردن این دو حوزهٔ شهروندی گردیده است. شهروندی دیجیتال هم فرصت‌های جدیدی برای مشارکت مدنی، سیاسی و اجتماعی، به‌ویژه از راه رسانه‌های اجتماعی و دیگر فناوری‌های تعاملی فراهم کرده است (کیتینگ،[2] ۲۰۱۶). شهروندی دیجیتال، به‌کارگیری مسئولانهٔ فناوری برای فعالیت‌هایی چون یادگیری، ساخت و مشارکت است که به داشتن مهارت‌های منحصربه‌فرد نیاز دارد (جیمز[3] و همکاران، ۲۰۲۱).

نمونه‌هایی از حقوق و مسئولیت‌های شهروندی درزمینهٔ امنیت را می‌توان در همهٔ ابعاد شهروندی پیدا کرد. برای نمونه می‌توان به امنیت جانی، مالی و تجارت، حساب‌های بانکی و معاملات اشاره کرد که برآورده کردن آن بر عهدهٔ نهاد قضایی، پلیس و نیروهای مسلح است و در حیطهٔ شهروندی سنتی سیاسی، مدنی و اجتماعی قرار دارد. امنیت در ابعاد امروزی‌تر شامل پایداری در مسائل اجتماعی، فرهنگی و اقتصادی کلان است که امنیت در آن‌ها به عهدهٔ نهادهای مدنی و سیاسی جامعه است (هادی‌سیفی و همکاران، ۱۳۹۸)؛ همچنین امنیت محیط زندگی شهری (بهداشت و سلامت، آموزش، نگهداری، تعمیر و ساخت راه‌های ارتباطی) و طبیعت که به‌ترتیب بر عهدهٔ پلیس و سازمان جنگل‌ها و مراتع و محیط‌زیست است و در ابعاد شهروندی زیست‌محیطی و توسعهٔ پایدار مورد توجه قرار می‌گیرند (امیری و احدنژاد، ۱۳۹۷).

1. Xu
2. Keating
3. James

علاوه‌بر این، امروزه بُعد نوین شهروندی آنلاین یا دیجیتال که به رفتار مسئولانه، قانونی و ایمن شهروندان یا استفادهٔ مناسب از فناوری و انتخاب‌های ایمن، مسئولانه و محترمانهٔ آنلاین اشاره دارد، مطرح شده است (جونز و میشل،[1] ۲۰۱۵). فناوری مدرن و علم نوین سبب پیدایش انواع جدید جرائم شده است که درنتیجهٔ آن پلیس تخصصی فتا (فضای تولید و تبادل اطلاعات) با هدف تأمین امنیت فضای مجازی، حفظ آزادی‌های مشروع، حفظ امنیت شهروندان و حفظ زیرساخت‌های کشور در برابر حمله‌ها و جرم‌های سایبری ایجاد و تشکیل شده است تا پیگیر برقراری امنیت در این حوزه باشد (امیریان‌فارسانی و همکاران، ۱۳۹۶). همان‌طور که فناوری به‌طور یکپارچه در هر گوشه از زندگی روزمرهٔ ما پیشرفت می‌کند، حریم خصوصی و حفاظت از اطلاعات شخصی به‌طور جدایی‌ناپذیری در هم تنیده می‌شوند. امروزه امنیت دیجیتال، تنها به شیوهٔ مدیریت خطرات امنیتی اینترنتی بستگی ندارد، بلکه به این بستگی دارد که اقدامات و رفتار ما دیگران را در معرض خطر قرار ندهد. بنابراین، شهروند دیجیتال بودن به این معناست که افراد بیاموزند چگونه از دسترسی به دستگاه‌های خود محافظت کنند و از هرچیزی که می‌تواند حریم خصوصی و امنیت را تهدید کند، با احتیاط استفاده کنند.

۳. ضرورت آموزش ابعاد شهروندی نوین

در آموزش شهروندی، افراد جامعه می‌آموزند که به گزارش‌دهی جرمی که شاهد آن هستند، اولویت داده و بدانند چگونه به تهدیدهایی که با آن‌ها روبه‌رو می‌شوند، پاسخ دهند و با احتیاط با دنیای خود تعامل کنند. به‌این‌ترتیب شهروندان با در نظر داشتن مسئولیت مشترک برای افزایش شناخت و آگاهی، اِعمال حقوق و مسئولیت‌های شهروندی، به مقامات دولتی در برقراری امنیت کمک می‌کنند. همچنین برای پیشگیری از رفتار مجرمانه و پرخطر، خودگردانی و تشخیص موقعیت‌های پرخطر آموزش داده می‌شود تا بتوانند پیش از درگیری در چنین موقعیت‌هایی، از خود محافظت کنند. شهروندان باید بتوانند پیش از اینکه دیر شود علائم جنایت را تشخیص دهند و قبل از ظهور پیامدهای

1. Jones & Mitchell

خشونت‌آمیز خطر را پیش‌بینی کنند. همچنین بر اهمیت ایجاد فضایی برای همکاری و تضمین امنیت تأکید می‌شود که به کاهش فرصت‌های خشونت و بزهکاری کمک می‌کند (امرسون،[1] ۲۰۲۰).

اگر قرار است اینترنت همانند دنیای واقعی، محیطی برای اعتماد باشد، که در آن حقوق اساسی بشر و ذهنیت مدنی حاکم باشد، آموزش افراد جامعه در این زمینه یک اولویت است (ریچاردسون و میلویدو،[2] ۲۰۱۹). مسائل امنیتی در استفاده از فناوری آنلاین که برای محافظت از خود مصرف‌کننده در نظر گرفته می‌شوند، نیازمند دانش و مهارت‌هایی برای انجام اقدامات احتیاطی در برابر استفاده از دستگاه‌های الکترونیکی دیجیتال است. کاربران، مسئول حفظ ایمنی و رفاه خود هستند و باید اقداماتی مانند نصب و به‌روزرسانی نرم‌افزار آنتی‌ویروس، نصب و به‌روزرسانی نرم‌افزار ضدجاسوسی و خاموش کردن فایروال‌ها را که ازجمله اقدامات امنیتی هستند، بدانند. این اقدامات برای محافظت از اطلاعات دیجیتال در برابر سرقت یا آسیب دیدن ضروری هستند (ماهادیر[3] و همکاران، ۲۰۲۱) و در آموزش شهروندی دیجیتال در نظر گرفته می‌شود و شامل حریم خصوصی و امنیت، روابط و ارتباطات، آزار و اذیت سایبری، ردپای دیجیتال، شهرت، تصویر و هویت از خود، سواد اطلاعاتی، و رفتار اخلاقی و رعایت قوانینی مانند کپی‌رایت است که همه به‌نوعی به حوزهٔ امنیت مربوط می‌شوند (جونز و میشل، ۲۰۱۵)

بنابر آنچه گفته شد، اگر نهاد قضایی و پلیس اجتماعی و سایبری تمایل دارد از آسیب‌های اجتماعی پیشگیری کرده، آمار جرائم را کاهش دهد، باید قانون‌گرایی را افزایش دهد که از بهترین راه‌های آن، آموزش شهروندی است که در آن افراد جامعه با حقوق و مسئولیت‌های خود به‌عنوان افراد جامعه آشنا می‌شوند. آموزش شهروندی و شکل‌گیری محیط‌های فرهنگی می‌تواند نقش مهمی در ترویج افشای تخلفات ایفا کند. محیطی که از ارزش‌های پاسخ‌گویی، شفافیت و حاکمیت قانون و افشاگران تخلف‌ها حمایت کند،

1. Emerson
2. Richardson & Milovidov
3. Mahadir

پیش‌نیاز جامعه‌ای امن است. همچنین آگاهی از اینکه نهاد امنیتی کشور موظف‌اند که گزارش‌های مربوط به تخلفات مشکوک را بررسی کرده و در صورت نیاز اقدام نموده و از افشاگر حفاظت کنند، به اقدام کردن شهروندان کمک کرده، آن‌ها را برای مشارکت فعال تشویق می‌نماید (لویز و کستلینو،[1] ۲۰۱۳).

در ادامهٔ این مقاله به برخی از جرائم و آسیب‌های امنیتی نوین در دنیای دیجیتال که در آموزش شهروندی مورد توجه‌اند، اشاره می‌شود.

۴. خطرها و آسیب‌های نوین در دنیای دیجیتال

خطرهای موجود در دنیای آنلاین یا دیجیتال شامل موارد زیر است که در آموزش‌های شهروندی دیجیتال به آن توجه می‌شود:

۴ـ۱. خطر حفظ حریم خصوصی

ما در عصر داده‌های بزرگ زندگی می‌کنیم؛ جایی که اطلاعات خصوصی سرمایه است. شهروندان باید در فعالیت‌های آنلاین خود، به‌ویژه در رسانه‌های اجتماعی و هنگام استفاده از موتورهای جست‌وجو، در نظر داشته باشند که هم مصرف‌کننده و هم محصول هستند. هم سایت‌های تجاری و هم سایت‌ها و پلتفرم‌های غیرتجاری، محتوایی را استفاده کرده، براساس ردپایی که به‌صورت آنلاین به جا می‌گذاریم، سایت‌ها و تبلیغات را برایمان سفارشی می‌کنند (چوی[2] و همکاران، ۲۰۲۱).

اگرچه در دنیای امروز، حفظ قدرت کامل شهروندان بر داده‌های شخصی‌شان یک شاهکار تقریباً غیرممکن است، آموزش شهروندی می‌تواند با پرورش مهارت‌های مناسب به این امر کمک شایانی نماید. برای نمونه، درک شرایط و ضوابط ارائه‌دهندگان خدمات اطلاعات و هدف کوکی‌ها قبل از رضایت با آن‌ها، در شهروندی دیجیتال ضروری است. شهروندان همچنین باید بتوانند تصمیم بگیرند که چه زمانی داده های مورد درخواست را

1. Lewis & Castellino
2. Choi

ارائه کنند یا نه، هدف و استفادهٔ نهایی از جمع‌آوری داده‌ها را تأیید کنند، و مطمئن شوند که اطلاعات جمع‌آوری‌شده چگونه پردازش می‌شوند. آن‌ها باید بدانند چگونه، چه زمانی و کجا می‌توانند دسترسی به داده‌های شخصی را بپذیرند، از جمع‌آوری آن‌ها بدون رضایت آگاهانه خودداری کنند، آن‌ها را اصلاح، حذف یا پاک کنند. شهروندان باید بدانند که چگونه با ارائه‌دهندگان خدمات تماس بگیرند و در صورت نقض حقوقشان از سازمان ملی حفاظت از داده‌ها (پلیس فتا) کمک بگیرند (ریچاردسون و میلویدو، ۲۰۱۹).

سرقت هویت: به دست گرفتن و استفاده از هویت الکترونیکی دیگران (مانند نام کاربری و رمز عبور) برای ارتکاب کلاهبرداری و بهره‌مندی از آن است. با افزایش تعداد افراد آنلاین و به‌ویژه کسانی که از خدمات شخصی‌سازی‌شده استفاده می‌کنند، تعداد هویت‌های مجازی درحال افزایش است و سرقت هویت، خطری فزاینده شده است (چوی و همکاران، ۲۰۲۱).

افشای اطلاعات خصوصی: هنگام تنظیم یا ایجاد یک نمایه در یک پلتفرم اجتماعی، از کاربران دعوت می‌شود تا اطلاعات خصوصی خود را ارائه کنند. همچنین در اتاق‌های گفت‌وگو و انجمن‌ها، ممکن است کاربران داده‌های خصوصی مانند آدرس یا شماره تلفن خود را برای دیگران فاش کنند (ویلسون[1] و همکاران، ۲۰۱۱). بسیاری از کاربران از اتصال بی‌سیم رایگان موجود در کافه‌ها، رستوران‌ها و دیگر مکان‌های عمومی استفاده می‌کنند و اطلاعات شخصی و مالی را در این محیط‌ها ارائه می‌دهند (چوی و همکاران، ۲۰۲۱).

تور انداختن:[2] به فرایند جمع‌آوری اطلاعات بانکی، به‌ویژه شماره‌های شناسایی شخصی و شماره‌های احراز هویت تراکنش، با هدف غارت حساب‌های بانکی دیگران اشاره دارد. افراد ناآگاه نمی‌توانند یک وب‌سایت جعلی را تشخیص دهند، درنتیجه به‌راحتی اطلاعات بانکی خود را ارائه می‌دهند (ویلسون و همکاران، ۲۰۱۱). این واژه از کمین برای رمزهای عبور نشئت می‌گیرد و یکی از اشکال سرقت هویت است. برای

1. Wilson
2. Phishing

نمونه، گیرندگان هرزنامه‌ای دریافت می‌کنند و آن را نامه‌ای قانونی از یک مؤسسهٔ شناخته‌شده مانند یک بانک یا یک شبکهٔ اجتماعی معتبر در نظر می‌گیرند. این ایمیل‌ها اغلب حاوی پیوندهایی به وب‌سایت‌های جعلی هستند که برای جمع‌آوری اطلاعات حساس کاربر مانند شماره کارت اعتباری یا رمز عبور استفاده می شوند. اطلاعات هویتی به‌سرقت‌رفته اغلب برای ارتکاب کلاهبرداری استفاده می‌شود (ریچاردسون و همکاران، ۲۰۱۷).

تقلب تجاری: کلاهبرداری تجاری زمانی اتفاق می‌افتد که فروشندگان تظاهر به فروش کالا یا خدماتی کنند که پس از پرداخت، کالای آن‌ها یا ویژگی‌های وعده داده‌شده را ندارد و یا اصلاً کالا یا خدمات مورد نظر تحویل نمی‌شوند. همچنین می‌تواند ناشی از سرقت هویت و سرقت آنلاین فیشینگ باشد. یکی دیگر از منابع تقلب تجاری می‌تواند فروش خدمات دیجیتالی با قیمت غیرمنصفانه باشد (ویلسون و همکاران، ۲۰۱۱).

کلاهبرداری اینترنتی: در چند سال گذشته بسیار توسعه یافته، زیرا امکانات تجارت الکترونیک و پرداخت آنلاین چند برابر شده است. کلاهبرداری اینترنتی انواع مختلفی از کلاهبرداری مانند تقلب، کلاهبرداری در املاک، زنگ‌های پیامک خدمات برتر، کلاهبرداری در انتقال پول و... را شامل می‌شود (سان[1] و همکاران، ۲۰۲۱).

برای پیشگیری از گرفتار شدن در دام تبلیغات، شیوه‌های تجاری غیراخلاقی و اتلاف بیش از حد اطلاعات، شهروندان دیجیتال باید مهارت‌های تفکر انتقادی و تجزیه و تحلیل قوی را توسعه دهند. ابزارهای فیلتر و مسدود کردن تبلیغات وجود دارند، اما به‌ندرت کاملاً قابل اعتمادند، و اگر افراد جوان فهرستی از اقدامات برای اجتناب یا حذف سریع محتوای ناخواسته در اختیار داشته باشند، می‌توانند مفید باشد. این فعالیت آموزشی ارزشمند، گامی برای ایجاد مهارت‌های تفکر انتقادی است (ریچاردسون و میلویدو، ۲۰۱۹).

1. Sun

کوکی‌ها:[1] فایل‌های متنی هستند که هنگام بازدید از یک وب‌سایت در رایانه باقی می‌مانند. به رایانه آسیب نمی‌زنند، اما به اطلاعات مربوط به رفتار و علایق فرد دسترسی پیدا می‌کند. ازآنجاکه کوکی‌ها می‌توانند برای ردیابی الگوهای استفاده و اطلاعات تماس استفاده شوند، امکان تجاوز به حریم خصوصی را فراهم می‌کنند. آن‌ها همچنین هدف‌گیری رفتاری ازسوی تبلیغ‌کنندگان را ساده می‌کنند (ریچاردسون و همکاران، ۲۰۱۷).

بدافزار:[2] یک اصطلاح کلی است که برای اشاره به انواع مختلفی از نرم‌افزارهای متخاصم یا مزاحم، که شامل ویروس‌ها، اسب‌های تروجان و... استفاده می‌شود. اهداف بدافزار بسیار متنوع است. آن‌ها می‌توانند صرفاً با آسیب رساندن به نرم‌افزار یا خراب کردن سخت‌افزار، عملکرد رایانه را مختل کنند، یا ممکن است اطلاعات و داده‌هایی را سرقت کنند که به‌نوعی باعث کسب درآمد شود. رایانهٔ آلوده نیز ممکن است به یک ربات تبدیل شود که بدون اطلاع توسط مجرمان کنترل شود. سپس ممکن است همراه با میلیون‌ها کامپیوتر آلودهٔ دیگر به‌عنوان بخشی از یک بات‌نت برای انتشار هرزنامه، ارتکاب کلاهبرداری، یا انجام حملات علیه بیمارستان‌ها، فرودگاه‌ها یا بانک‌ها استفاده شوند (اسلان و سامت،[3] ۲۰۲۰).

هرزنامه:[4] به ارسال انبوه پیام‌های ناخواسته به چندین گیرنده اشاره دارد. معمولاً با ایمیل مرتبط است، اما در شبکه‌های اجتماعی، پیام‌های فوری، تلفن‌های همراه و... نیز کاربرد دارد. خوشبختانه اکثر سرویس‌های ایمیل دارای فیلترهای هرزنامهٔ کارآمد هستند. هرزنامه همچنین ممکن است به‌عنوان یک بردار برای انتشار انواع مختلف بدافزار عمل کند؛ برای مثال، زمانی که گیرنده یک پیوست یا پیوندی را که در نامهٔ هرزنامه مشخص شده است، باز می‌کند (کریم و همکاران، ۲۰۱۹).

1. Cookies
2. Malware
3. Aslan & Samet
4. Spam

هرزنامه، ویروس‌ها، بدافزارها و ربات‌ها، عواقب گسترده‌ای دارند و شهروندان دیجیتال اگر بدانند ابزارهای حفاظتی مناسب را از کجا تهیه کنند و چگونه از آن‌ها استفاده کنند، می‌توانند از خود در برابر این تهدیدات محافظت کنند. امنیت ناکافی گردش هرزنامه‌ها را آسان می‌کند. هرزنامه از رایج‌ترین ابزارهای انتشار اطلاعات نادرست یا تقلبی و سوءاستفاده از حسن نیت گیرندگان برای جمع‌آوری اطلاعات یا کسب سود مالی است. هر روز صدها ویروس و بدافزار جدید درحال ظهورند؛ بنابراین کاربران باید هر زمان که نسخه‌ها یا وصله‌های جدید در دسترس قرار می‌گیرند، در مورد به‌روزرسانی منظم امنیت خود کوشا باشند. تنظیمات مکان جغرافیایی و بلوتوث، در صورت مورد نیاز نبودن باید خاموش شوند، زیرا دسترسی آسان به مزاحمان را فراهم می‌کنند (ریچاردسون و میلویدو، ۲۰۱۹).

نمایه‌سازی: با افزایش تعداد نمایه‌هایی که یک فرد در پلتفرم‌های مختلف منتشر می‌کند، خطر اینکه داده‌های شخصی منتشرشده در یک پلتفرم با داده‌های دیگر پلتفرم‌های ادغام شوند یا در جاهای دیگر ارائه شوند (مثلاً در نظرسنجی یا قرعه‌کشی) افزایش می‌یابد. بنابراین پروفایل‌هایی ایجاد می‌شود که امکان مخاطب قرار دادن مستقیم افراد با محتوا، خدمات و تبلیغات ناخواسته را فراهم می‌کند. برای نمایه‌سازی می‌توان از وب‌سایت کمک گرفت، اما روش خطرناک‌تر زمانی است که نمایه‌های کاربران (یا نمایه‌های جزئی آن‌ها) از پایگاه دادهٔ پشت وب‌سایت جمع‌آوری می‌شود و توسط ارائه‌دهندهٔ پلتفرم به اشخاص ثالث فروخته می‌شود (ویلسون و همکاران، ۲۰۱۱).

یکی از عناصر مهم آموزشی در مورد حریم خصوصی، باید مفهوم پروفایل و پیوند دادن عناصر پراکنده اطلاعات در مورد یک شخص برای استنباط تصویر دقیق‌تری از او باشد. مفهوم آموزشی مهم این است که با کنار هم قرار دادن اطلاعات از سایت‌ها و شبکه‌های مختلف هویت فرد مشخص می‌شود (ریچاردسون و همکاران، ۲۰۱۷).

اینترنت اشیا:[1] توانمندی نظارت و کنترل از راه دور، موج نوینی از نوآوری‌ها را ارائه کرده که چگونگی نظارت بر فعالیت‌های گوناگونی مانند ردیابی کالا، مدیریت دارایی‌های فیزیکی، نظارت و کنترل بر سلامت و امنیت تجهیزات، ساختمان‌ها و افراد و دیگر موارد ایجاد کرده است. همچنین این نوآوری تهدیدهایی را در مباحثی مانند ردیابی، شناسایی، محرمانه بودن، دسترسی‌پذیری، شنود، سرقت اطلاعات، تعیین و سرقت هویت و حریم خصوصی ایجاد کرده است (رمضانی و موحدی‌صفت، ۱۴۰۰).

اتصال به اینترنت در اسباب‌بازی‌ها و وسایل خانگی که در بازار توزیع می‌شوند، نگرانی‌های اخلاقی را در میان مدافعان حقوق بشر ایجاد کرده‌اند. عروسک‌ها، ربات‌ها و دیگر انواع دستگاه‌های متصل می‌توانند درونی‌ترین ایده‌ها و افکار کودک را ضبط کنند و اگر اقدامات امنیتی به‌اندازهٔ کافی قوی نباشد، می توان به آن اطلاعات دسترسی و توسط اشخاص ثالث استفاده شود. درک و مراقبت از محیط دیجیتال ما به‌اندازهٔ مراقبت از خانه و محیط زندگی مهم است؛ به ویژه که اینترنت اشیا و اینترنت اسباب‌بازی‌ها راه خود را به زندگی روزمرهٔ ما باز کرده‌اند. خانه‌های متصل به وای‌فای، اسباب‌بازی‌ها و در آیندهٔ نزدیک، اتومبیل‌ها و وسایل حمل‌ونقل عمومی، به‌سرعت امنیت را به یک جنبهٔ بسیار مهم از زندگی ما تبدیل می‌کنند. خانواده‌ها باید از قابلیت‌های دستگاه‌های خانگی متصل به اینترنت، اینکه اطلاعات جمع‌آوری‌شده به کجا می‌روند، آگاه باشند. چه کسی فکرش را می‌کرد که تلفن همراه سرعت حرکات ما را ردیابی کند و همچنین به ما اطلاع دهد که چند کیلومتر در روز پیاده‌روی کردیم، یا اینکه مانیتورهای کودک همهٔ فعالیت‌های خصوصی او را گردآوری کند (ریچاردسون و میلویدو، ۲۰۱۹)؟!

مکان‌یابی جغرافیایی فرایند شناسایی مکان یک شیء است. برنامه‌های مکان‌یابی موقعیت مکانی شما را به کاربران گزارش می‌دهند. موقعیت جغرافیایی می‌تواند تهدیدی برای حریم خصوصی باشد، زیرا مکان فرد را مشخص می‌کند که برای برخی مانند کودکان می‌تواند تهدید باشد (ریچاردسون و همکاران، ۲۰۱۷).

1. Internet of things

در شهروندی دیجیتال، قانون‌های طلایی آموزش داده می‌شود؛ ازجمله این آموزش‌ها عبارت‌اند از: تبلیغات و ردیابی، کوکی‌های شخص ثالث، دسترسی به موقعیت مکانی خود را مسدود کنند و اطلاعات شخصی خود را با کسی که نمی‌شناسند و به آن اعتماد ندارند، به اشتراک نگذارند؛ از اطلاعات شخصی یا عکس شخص دیگری بدون رضایت او استفاده نکنند؛ از سیستم خود نسخهٔ پشتیبان تهیه کنند و یک خط‌مشی پشتیبان‌گیری منظم داشته باشند؛ از گذرواژه‌های قوی برای محافظت از رایانه، ایمیل و اتصالات اینترنتی خود استفاده کنند؛ پیش از ارائهٔ داده‌های خصوصی، نماد قفل‌شده (نشان دهندهٔ یک اتصال امن) را که در نوار ابزار نشان داده می‌شود، بررسی کنند؛ قبل از انجام معاملات آنلاین، بررسی کنند که URL شامل HTTPS باشد؛ از خرید آنلاین در وب‌سایت‌های غیرقابل اعتماد خودداری کنند؛ از افشای اطلاعات شخصی در وب‌سایت‌هایی با سطوح امنیتی پایین خودداری کنند؛ حتماً حقوق خود را بررسی کنند و توجه داشته باشند که به‌عنوان کاربر، مسئول انجام اقدامات احتیاطی در هنگام انتخاب مدرک یا سایر برنامه‌های آموزش از راه دور هستند؛ به قوانین اخلاقی همچون کپی‌رایت احترام بگذارند و از فیلتر کردن برای شناسایی و مسدود کردن پلتفرم‌ها و/یا محتوای نامناسب در اینترنت استفاده کنند (هید[1] و همکاران، ۲۰۱۷).

امنیت سایبری اجتماعی:[2] امنیت سایبری (عوامل انسانی است که از فناوری برای هک کردن فناوری استفاده می‌کند و هدف آن سیستم‌های اطلاعاتی است) هرچند مفهومی نوین است، زیرشاخه‌ای تازه‌تر به نام امنیت سایبری اجتماعی دارد که از فناوری به‌عنوان میانجی هک کردن شهروندان یا همان کاربران رسانه‌های اجتماعی استفاده می‌کند و با دست‌کاری اطلاعات، بر افکار عمومی اثر می‌گذارد. رسانه‌های اجتماعی ابزاری برای جنگ اطلاعاتی شده‌اند. پروپاگاندای رسانه‌ای به‌معنای بیان و بازنمایی گزینشی واقعیت‌ها به‌گونه‌ای است که واکنش و رفتار احساسی ازسوی مخاطب شکل دهد. پخش یا ترویج اطلاعات جانب‌دارانه سبب گمراهی مخاطب ناآگاه می‌شود. در رسانه‌ها راهنمایی‌های نادرست،

1. Hesd
2. Social Cybersecurity

روایت‌سازی از راه ترند کردن،[1] هشتک‌های چفت‌شده[2] (پیوند محتوای هشتک‌شده به موضوع‌های بی‌ربط)، پنهان‌سازی در دود[3] (پخش محتوا برای پنهان کردن محتوای مورد توجه روز)، محتواربایی[4] (گرفتن بخشی از پیام و تغییر به آنچه مد نظر است) و تعمیم روایت‌های نادرست[5] و بسیاری دیگر از روش‌های گمراه‌سازی انجام می‌شود (محمدی خانقاهی و آزادی، ۱۴۰۰).

شهروندان دیجیتال باید از خطرات فیزیکی نهفته در استفاده از فناوری آگاه باشند؛ اما بُعد دیگر آن مخاطرات جسمانی و روانی است که ممکن است در پی استفادهٔ بیش از اندازه از دستگاه‌های دیجیتالی ایجاد شود (ماهادیر و همکاران، ۲۰۲۱).

۴ـ۲. امنیت در بهزیستی و سلامت جسمانی

شهروندان به مجموعه‌ای از رفتارها، مهارت‌ها، ارزش‌ها و درک نیاز دارند که آن‌ها را از چالش‌های مربوط به سلامت و تندرستی کاملاً آگاه کند.

۴ـ۳. رفتار ایمن مرتبط با سلامت جسمانی

آموزش رفتار فردی درست در استفاده از ابزارهای نوین برای حفظ سلامت شهروندان ضروری است. این‌گونه رفتارها، اختلالات مربوط به اعصاب ناشی از استفاده از رایانه را کاهش می‌دهد. برای نمونه، شهروندان باید بیاموزند هنگام استفاده از رایانه از یک صندلی قابل تنظیم استفاده کنند تا مطمئن شوند که تمرکز چشم‌ها موازی با صفحهٔ رایانه است و در فاصلهٔ مناسب قرار دارند (ماهادیر و همکاران، ۲۰۲۱). به‌دلیل کاهش خواب ناشی از دوزهای بیش از حد نور آبی، چند ساعت پیش از زمان خواب استفاده از ابزارهای الکترونیک را کاهش دهند. نکات دیگری نیز ذهن متخصصان بهداشت و درمان را به خود مشغول داشته است؛ ازجمله اینکه انفجار اطلاعات به‌صورت صوتی و تصویری می‌تواند

1. Narrative creation by Trend
2. Hashtag latching
3. Smoke screening
4. Thread jacking
5. False generalized other

باعث رشد بیش از حد بخش‌های خاصی از مغز و کند کردن رشد در قسمت‌های دیگر شود. برای نمونه، در بررسی‌ها به رشد ناکافی لوب جلوی مغز توجه شده است که سبب کاهش تمرکز و تأخیر در رشد مهارت‌های هماهنگ حرکتی خاص می‌شود. تحقیقات انعطاف‌پذیری عصبی نشان می‌دهد که تحریک بیش از حد مداوم مغز ما ناشی از انبوه صداها و تصاویر سریعی که از طریق اینترنت با آن‌ها بمباران می‌شویم، بر ظرفیت پردازش نشانه‌های غیرکلامی و دیگر نشانه‌های ظریف در تعامل بین فردی تأثیر می‌گذارد (ریچاردسون و میلویدو، ۲۰۱۹).

همچنین با توجه به اطلاعات بهداشتی فراوان و اغلب گمراه‌کننده‌ای که در فضای مجازی پخش می‌شوند، شهروندان باید مهارت‌هایی چون تفکر انتقادی برای تشخیص درست از نادرست را بیاموزند تا درگیر مشکلات ناشی از این اطلاعات نشوند. برای نمونه، تمرکز بر زیبایی و تناسب بدن در عصر سلفی و لایک‌های امروزی می‌تواند به‌سرعت جوانان را به‌سمت تغذیهٔ نادرست و اختلالات خوردن مانند بی‌اشتهایی سوق دهد. این چالش‌ها احتمالاً تأثیر پایداری بر زندگی اجتماعی، حرفه‌ای و عاطفی افراد و درنتیجه بر نقش آن‌ها به‌عنوان یک شهروند فعال خواهند داشت (پدین[1] و همکاران، ۲۰۲۱).

۴ـ۵. رفتار ایمن مرتبط با سلامت روانی

ساعت‌های طولانی استفاده از اینترنت می‌تواند بر تحصیل جوانان، تعاملات خانوادگی و بهزیستی روانی تأثیر منفی بگذارد. دور شدن از تعاملات اجتماعی رودررو، فعالیت بدنی کم، مشکلات تحصیلی، تحریک‌پذیری و مشکلات خواب ایجاد می‌کند. یافته‌های پژوهش‌ها در این زمینه نشان دادند که استفادهٔ بیمارگونه از اینترنت با بیش‌فعالی/ بی‌توجهی، مشکلات رفتاری، افکار و اقدام به خودکشی مرتبط است؛ افسردگی، اضطراب و مشکلات ارتباط با همسالان را افزایش می‌دهد؛ همچنین وسواس (وسواس در استفاده از اینترنت)، غفلت (بی‌توجهی به فعالیت‌های دیگر) و اختلال کنترل (ناتوانی در کنترل/

1. Padín

محدود کردن استفاده از اینترنت) را به وجود می‌آورد (ونگ،[1] ۲۰۲۰). قرار گرفتن در معرض رسانه‌های اجتماعی/اینترنت پتانسیل تقویت افکار و رفتارهای منفی را دارد (سدویک[2] و همکاران، ۲۰۱۹). استفادهٔ بیش از حد از اینترنت با یک وضعیت روان‌پزشکی به نام اعتیاد به اینترنت مرتبط است. به‌تازگی، در ویرایش پنجم *راهنمای تشخیصی و آماری اختلالات روانی (DSM-5)*، اختلال بازی اینترنتی به‌عنوان یک تشخیص جدید گنجانده شده است. اعتیاد به اینترنت، خطر مشکلات روانی همچون افسردگی، احساس تنهایی و تمایل به خودکشی را افزایش داده است (مالینوسکاس و مالینوسکسنه،[3] ۲۰۱۹). پژوهش‌ها نشان داند قربانی سایبری شدن با اقدام به خودکشی همراه است (سدویک و همکاران، ۲۰۱۹). کسانی که به‌صورت آنلاین مورد سوءاستفاده قرار گرفته‌اند، ۲/۳ برابر بیشتر درگیر رفتارهای خود آسیب شدند و ۲/۵ برابر بیشتر اقدام به خودکشی کردند (هریسون و پلیزی،[4] ۲۰۲۲).

نوجوانان با صلاحیت اجتماعی ضعیف که از مشکلات روانی اجتماعی (مانند افسردگی، اضطراب اجتماعی و تنهایی) رنج می‌برند یا ممکن است به‌طور غیرعادی نگران تعاملات اجتماعی باشند، به‌دلیل ناشناس بودن در اینترنت و پوششی که برای برقراری روابط در شرایط کم‌خطرتر در اختیار می‌گذارد، به دنیای مجازی کشیده می‌شوند (مالینوسکاس و مالینوسکسنه، ۲۰۱۹). آزار و اذیت سایبری و سکستینگ[5] (اقدام به ارسال عکس‌ها یا پیام‌های جنسی صریح ازطریق تلفن همراه) ریشه‌های پیچیده‌ای در شکل‌گیری هویت نوجوانان، مبارزات همسالان، عزت نفس، کاوش‌های عاشقانه و تصمیم‌گیری جنسی دارند (جونز و میشل، ۲۰۱۵). گرایش به سلفی گرفتن برای به دست آوردن توجه دیگران، دانش و درک فرد از خود را از بین می‌برد. افراد زندگی واقعی خود را براساس

1. Wong
2. Sedgwick
3. Malinauskas & Malinauskiene
4. Harrison & Polizzi
5. sexting

ایدئال‌ها و گرایش‌های رایج پخش‌شده در دنیای مجازی تنظیم می‌کنند و به‌جای شکل دادن به دنیای مجازی، شکل آن را به خود می‌گیرند (ریچاردسون و میلویدو، ۲۰۱۹).

اینترنت رویارویی بین افراد هم‌فکر را تسهیل می‌کند و می‌تواند با گرد هم آوردن افرادی که قبلاً انواع خاصی از رفتارهای انحرافی را پنهان می‌کردند، تأثیر عمده‌ای بر اخلاقیات بگذارد، زیرا توسط جامعه پذیرفته نشده بود. وقتی چنین گروه‌هایی بتوانند باهم ملاقات کنند و تجربیات خود را به اشتراک بگذارند، بایدهای اخلاقی کم‌رنگ شده و اعمال انحرافی آن‌ها می‌تواند قابل قبول به نظر برسد، زیرا افراد زیادی آن را انجام می‌دهند. یک نمونهٔ بازار بسیار سودآور، سوءاستفادهٔ جنسی از کودکان و دیگری، سخنان نفرت‌انگیز و افراط‌گرایی است. شهروندان دیجیتال باید اهمیت وفاداری به اخلاقیات خود را درک کنند و آگاه باشند که نباید تنها به این دلیل که بسیاری کاری را انجام می‌دهند، استانداردهای اخلاقی خود را زیر پا بگذارند. جست‌وجو برای مطالب خاص از روی کنجکاوی می‌تواند به‌سرعت توسط سازوکارهای فیلترینگ و پروفایل رسانه‌های اجتماعی و ارائه‌دهندگان اخبار انتخاب شود و جوانان را به برخوردهای ناخواسته سوق دهد (چان[1] و همکاران، ۲۰۲۲).

ناشناس بودن زمینه‌ساز بسیاری از چالش‌ها و خطراتی است که از تعاملات آنلاین ناشی می‌شود و با مسئولیت‌پذیری همراه است. زمانی که کاربران اینترنت بر این باورند که نمی‌توان اعمالشان را ردیابی کرد، تمایل دارند به روشی بسیار متفاوت از آنچه در غیر این صورت انجام می دادند رفتار کنند. رفتار اخلاقی در موقعیت های به‌ظاهر ناشناس، تمرکز بسیار بیشتری بر ارزش های عدالت و انصاف دارد که به‌نوبهٔ خود بر پایهٔ احترام به کرامت انسانی و حقوق بشر، نگرش مدنی و نگرش مسئولانه و محترمانه به خود و دیگران است (هنل[2] و همکاران، ۲۰۱۹).

1. Chan
2. Hennell

۵. زورگویی یا قلدری شایع‌ترین رفتار مخل سلامت روان در دنیای دیجیتال

انواع مختلف قلدری همیشه بخشی از زندگی اجتماعی بوده، اما در دنیای مجازی به‌دلیل ناشناس بودن افزایش یافته است؛ به‌ویژه کودکان و جوانان در خطر قربانی قلدری و یا ارتکاب آن هستند. ازاین‌رو قلدری با رفتار خود فرد و همچنین رفتار دیگران مرتبط است. حتی انتشار محتوایی مانند تصاویر افتراآمیز می‌تواند بخشی از قلدری باشد (ویلسون و همکاران، ۲۰۱۱). قلدری یک مفهوم چتر و شامل موارد زیر است:

- **زورگویی سایبری**: ازطریق اینترنت یا تلفن همراه انجام می‌شود و شامل پیام‌ها یا ایمیل‌های توهین‌آمیز یا مخرب در اتاق گفت‌وگو یا وب‌سایت‌هاست که با هدف آسیب به یک فرد یا گروه خاصی از مردم فرستاده می‌شوند. زورگویان سایبری همچنین از تلفن‌های همراه برای گرفتن عکس‌های شرم‌آور استفاده می‌کنند. زورگویی آنلاین تأثیر بسیار بیشتری نسبت به زورگویی معمولی دارد؛ زیرا نویسندگان با احساس ناشناس بودن تقویت می‌شوند و قربانیان جایی برای پنهان شدن ندارند (ریچاردسون و همکاران، ۲۰۱۷).
- **آراستن**:[1] به پدوفیل[2]هایی گفته می‌شود که از اینترنت به‌عنوان وسیله‌ای برای تماس با کودکان و جوانان استفاده می‌کنند و درعین‌حال هویت بزرگسالی خود را پنهان می‌کنند. آن‌ها اغلب استراتژی خود را براساس اشتیاق کودکان به دوستی و آشنایی بنا می‌کنند. همهٔ مناطقی از اینترنت که بسترهایی را برای تماس و تبادل شخصی فراهم می‌کنند، احتمالاً مبنایی برای حملات آراستن فراهم می‌کنند. با افزایش فناوری‌های ارتباطی موبایل و شبکه‌های اجتماعی، خطر درگیر شدن در حمله‌های آزار جنسی و پذیرش یک دعوت خطرناک را افزایش داده است (ویلسون و همکاران، ۲۰۱۱).

1. Grooming
2. paedophiles

- **تعقیب مجازی:**[1] استفاده از اینترنت یا سایر ابزارهای الکترونیکی برای تعقیب یا آزار یک فرد، یک گروه یا یک سازمان است (قونی،[2] ۲۰۲۲).
- **تهدید مجازی:**[3] عمل ایجاد مشکل در اینترنت با شروع مشاجره یا ناراحت کردن افراد، با ارسال پیام‌های تحریک‌آمیز، خارج از موضوع در یک جامعهٔ آنلاین مانند گروه خبری یا وبلاگ است و با هدف عمدی برانگیختن خوانندگان به یک واکنش عاطفی یا ایجاد اخلال در بحث عادی دربارهٔ یک موضوع انجام می‌شود (ارتیز،[4] ۲۰۲۰).

قلدری و آزار و اذیت‌هایی مانند تعقیب و تهدید مجازی، روحیهٔ افراد را کاهش می‌دهد و فضای ترس و بی‌اعتمادی ایجاد می‌کند. برای کسانی که مورد آزار و اذیت قرار می‌گیرند یا قربانی آزار و اذیت می‌شوند، افسردگی، اضطراب، عزت نفس پایین، مشکلات سازگاری اجتماعی و تنهایی به دنبال دارد (دال‌کاسون[5] و همکاران، ۲۰۲۰).

برای مجرمان، شایع‌ترین اثرات شامل افزایش اضطراب و انجام رفتارهای بزهکارانهٔ بیشتر است (ریچاردسون و همکاران، ۲۰۱۷).

یکی از اقدامات پیشگیرانه برای کمک به جلوگیری از تبدیل شدن قلدری یا آزار و اذیت، این است که مدیریت روابط اجتماعی، مدیریت خشم و حل تعارض آموزش داده شود تا افراد استعدادهای خود را به‌عنوان میانجی‌های بالقوه در درگیری‌ها کشف کنند و به‌این‌ترتیب، خطر درگیری‌های جزئی که به رفتارهای تهدیدآمیز تبدیل می‌شوند، هم به‌صورت آفلاین و هم آنلاین کاهش یابد. به افراد آموزش داده می‌شود که ارتباط خود را با هرکسی که آن‌ها را آزار می‌دهد یا به هر نحوی در زمان آنلاین بودن آن‌ها را ناراحت می‌کند، قطع کنند. افراد بیاموزند چگونه سیگنال‌های قربانیان و همچنین شخص مسئول رفتار توهین‌آمیز را بخوانند و وقتی متوجه چنین سیگنال‌هایی می‌شوند چگونه واکنش

1. Cyberstalking
2. Goni
3. Trolling
4. Ortiz
5. Dal Cason

نشان دهند. باید چهار قانون طلایی برای مقابلـه بـا آزار و اذیـت سـایبری را آمـوزش داد: ۱. در صورت امکان از مطالب توهین‌آمیز کپی تهیه کنید؛ ۲. مطالـب تـوهین‌آمیـز را بـرای دیگران ارسال نکنید؛ ۳. دستگاه گیرنده (رایانه یا تلفن همراه) را خاموش کنید؛ ۴. حادثه را به یک بزرگسال مورد اعتماد یا مقام قضایی گزارش دهید (لنهارت[1] و همکاران، ۲۰۱۶).

کارکردهای آموزش شهروندی نوین در ایران

بابایی (۱۴۰۰) به نقل از رئیس‌پلیس فتای تهران بزرگ، جرم‌هـای نـوین را شـامل جـرائم حوزهٔ بانکداری الکترونیکی مثل کارت‌های بانکی، فیشینگ، اسکیمر، کلاهبرداری اینترنتی، باج‌گیری، هتک حرمت، توهین، هرزه‌نگاری، قمار و شـرط‌بنـدی آنلایـن، فـروش دارو و محصولات سلامت‌محور، فروش مواد مخدر و سلاح، نقض حریم خصوصـی و هرآنچـه که سلامت و امنیت روانی و اقتصـادی را در فضـای مجـازی تهدیـد مـی‌کنـد، دانسـت و بیشترین جرم‌ها را مربوط به کلاهبرداری مالی و اقتصادی (در سـال‌هـای اخیـر در حـوزهٔ ارزهای دیجیتال) معرفی کرد. همچنین فرستادن پیامک‌هـایی بـا نـام سـامانهٔ ثنـا یـا دیگـر ارگان‌های دولتی را که درخواست پول کرده یا دارای لینک بدافزارند، بسیار شـایع دانسـت (بابایی، ۱۴۰۰).

در آموزش شهروندی به‌جای ایجاد ترس یـا دادن پنـد بـرای جلـوگیری از رفتارهـای مشکل‌زا مانند آزار و اذیت سایبری و ارسال پیامک‌های توهین‌آمیز و ناخوشایند کـه تـأثیر چندانی بر کاهش این‌گونه مشکلات ندارند، بر آمـوزش و ایجـاد و تمـرین مهـارت‌هـای اجتماعی خاص تمرکز می‌شود. برنامه‌های شهروندی دیجیتالی که به افراد کمـک مـی‌کنـد اختلاف‌نظرها و بحث‌های آنلاین محترمانه را تمرین کرده و در فعالیت‌های مـدنی آنلایـن شرکت کنند، می‌توانند سبب کاهش رفتارهای آزار و اذیت آنلایـن و قربـانی شـدن افـراد شود. بررسی‌ها نشان دادند که راهبردهای مثبت و تعاملی در کاهش پرخاشگری جوانـان و مشکلات اجتماعی و عاطفی مرتبط با آن مؤثرتر بوده و بـه تقویـت نقـش تماشـاگران در حمایت از قربانیان و اعتراض در برابر رفتارهای نامناسب و کـاهش قلـدری کمـک کـرده

1. Lenhart

است (جونز و میشل، ۲۰۱۵). وجود تماشاگران نافعال می‌تواند بازخورد مثبتی را برای قلدر فراهم کند، زیرا قلدر و قربانی ممکن است این سکوت را تأییدی برای قلدری در نظر بگیرند (هریسون و پلیزی، ۲۰۲۲).

برای ایجاد نظم در استفاده از اینترنت، باید فرهنگ مؤدبانه و اخلاقی در دنیای دیجیتال آموزش داده شود و روش تعامل و ابراز وجود، کنترل شود تا هرج‌ومرج در فضای مجازی رخ ندهد. آموزش شهروندی می‌تواند با آموزش نتیکت[1] (اخلاق در دنیای دیجیتال) آداب در برقراری ارتباط در فضای مجازی را به شهروندان یاد داده، از درگیری‌های ناشی از بدرفتاری یا سوءتفاهم پیشگیری کند (سینتیا و ایپدواتی،[2] ۲۰۲۲). در آموزش شهروندی دیجیتال افراد می‌آموزند تصمیم‌گیری اخلاقی آنلاین درست داشته باشند. مانند اینکه به‌درستی تصمیم بگیرند آیا باید یک پست ناخوشایند را بازنشر کنند یا آن را به مقامات ذی‌صلاح گزارش کنند؛ یا یک عکس نامطلوب را به‌اشتراک بگذارند یا آن را حذف کنند (هریسون و پلیزی، ۲۰۲۲).

مورد دیگری که در آموزش شهروندی دیجیتال مورد توجه قرار می‌گیرد، همدلی است که عامل تعیین‌کنندهٔ مهمی در رفتار اخلاقی و یک عنصر ضروری در ایجاد اجتماعات اخلاقی است. درک ارزش‌های کرامت انسانی و حقوق بشر استوار است و با نگرش احترام به دیگران و احساس مسئولیت در برابر آن‌ها شکل می‌گیرد؛ همچنین ازطریق دانش قوی و درک انتقادی از خود شکل می‌گیرد. از همدلی می‌توان برای تحریک یا تقویت رفتار ضداخلاقی استفاده کرد. همدلی به افراد کمک می‌کند تا راحت‌تر در یک گروه یا زمینهٔ جدید قرار بگیرند، زیرا به آن‌ها ابزاری می‌دهد تا موقعیت را ارزیابی کنند و به‌گونه‌ای عمل کنند که پذیرفته شوند و درعین‌حال به ارزش‌های خود وفادار بمانند. اگر شهروندان آگاه باشند و به‌اندازهٔ کافی همدل باشند که بتوانند به مسائل از دیدگاه‌های مختلف نگاه کنند، بیشتر می‌توانند ابهام را تحمل کنند و کمتر تحت‌تأثیر همسالان، رسانه‌ها و روندها قرار می‌گیرند. آن‌ها می‌توانند بپذیرند که دیدگاه‌های گوناگون که در

1. netiquette
2. Sinthiya & Ipnuwati

کنار هم وجود دارند، می‌توانند عنصری غنی‌کننده و توانمند بدون نیاز به متقاعد کردن یا تبدیل کردن دیگران باشند (ریچاردسون و میلویدو، ۲۰۱۹).

آموزش شخصیت، فضیلت‌های انسانی و توسعهٔ خرد سایبری، بخشی از آموزش شهروندی دیجیتال است (هریسون و پلیزی، ۲۰۲۲). همچنین آموزش شهروندان با افزایش سطح آگاهی افراد جامعه به رشد جامعهٔ مدنی کمک می‌کند که به کمک نقش و جایگاه مردم و نهادهای اجتماعی به جرائم اینترنتی به شکل پیشگیرانه و فعال پاسخ می‌دهند (مشکین و همکاران، ۱۴۰۰). شهروندی دیجیتال به‌عنوان رفتار مناسب و مسئولانه در استفاده از فناوری دیجیتال که جزء مهم آموزش فناوری است، تعریف می‌شود (ذوالقدری[1] و همکاران، ۲۰۲۲). شهروندان می‌آموزند با گزارش دادن تخلف و اقداماتی مانند طرد یا مصرف نکردن یا حمایت از قربانی به شکل‌گیری محیط امن‌تر کمک کنند (مشکین و همکاران، ۱۴۰۰). پیدایش دنیای مجازی و شبکهٔ اطلاعات زمینهٔ انجام فعالیت‌های مجرمانهٔ تازه‌ای را فراهم کرده است. همچنین جرم‌های سنتی راهی نو برای انجام یافته‌اند (کردعلیوند و میرزایی، ۱۳۹۷). جریان جهانی شدن و توسعهٔ صنعت، جریانی از تغییرات دگرگونی دیجیتال را به ارمغان می‌آورد که بر تغییرات در نظم زندگی و رفتار مردم تأثیر می‌گذارد. جامعهٔ مجازی نیازمند مرجعی برای شناخت قوانین مربوط به محدودیت‌ها و امکانات اینترنت است. بنابراین آموزش نت‌اخلاق ضروری است تا راهنمایی برای رفتار مطابق با قوانین هنجاری وجود داشته باشد. همچنین اصول اخلاقی، در قانون اطلاعات و تراکنش‌های الکترونیک که نحوهٔ انجام تعاملات، ارتباطات و تراکنش‌ها ازطریق اینترنت و در صورت نقض تحریم‌ها را تنظیم می‌کند تا فضای اخلاقی برای استفاده از اینترنت ایجاد شود (پتوآنجی و ایپنوواتی،[2] ۲۰۲۲).

برای نمونه می‌توان به یک مورد تلاش برای سرقت که در پایان سال ۲۰۲۰، در دانشگاه ایالتی یوگیاکارتا رخ داد، اشاره کرد که یک ایمیل فیشینگ به دانشجویان ارسال شد که وانمود می‌کرد مدیر فناوری دانشگاه است و اطلاعات شخصی مانند ایمیل، رمز

1. Zulqadri
2. Putu Anggie & Ipnuwati

عبور و تاریخ تولد آن‌ها را درخواست کرده و تهدید می‌کرد در صورت ارسال نشدن اطلاعات خواسته‌شده، حساب کاربری آن‌ها بسته خواهد شد. مدیر فناوری اطلاعات و ارتباطات دانشگاه به‌سرعت درجریان قرار گرفت و توضیحی در مورد ایمیل فیشینگ ارائه کرد و از دانشجویان خواست پاسخ ندهند (ذوالقدری و همکاران، ۲۰۲۲).

ساری[1] و همکاران (۲۰۲۰) در پژوهش خود به این نتیجه رسیدند که خطر قلدری و کلاهبرداری اطلاعاتی برای دانش‌آموزان بسیار زیاد و اجتناب‌ناپذیر است. برای مقابله با خطرهای دیجیتالی نوین، آموزش شهروندی را در سه حوزهٔ سواد اطلاعاتی، سواد دیجیتال و سواد انسانی از نیازهای ضروری در جامعهٔ کنونی است. امرسون (۲۰۲۰) برای ایجاد محیط اجتماعی امن‌تر، مسئولیت‌پذیری را به شهروندان آموزش داد و برای این کار هنجارها و قوانین رفتاری و این را که چرا حاکمیت قانون در جامعه مهم است و چرا نقض می‌شود، آموزش داد. این آموزش به افراد امکان داد که رابطهٔ خود با قانون (چرا برای من مهم است) و رفتار قانونی را درک کنند. به‌این‌ترتیب کنترل رفتار قانونی از بیرونی به درون فردی تغییر کرد و رفتارهای مجرمانه را کاهش داد.

۶. نتیجه‌گیری و پیشنهادات

از بهترین راه‌های ایجاد قانون‌گرایی در جامعه و پیشگیری از جرائم سایبری یا قربانی شدن شهروندان، آموزش شهروندی است که در آن افراد جامعه با حقوق و مسئولیت‌های خود آشنا می‌شوند. همسو با نتایج این پژوهش در پژوهش کن (۲۰۲۴) و ماهر (۲۰۲۴) از آموزش شهروندی برای ایجاد امنیت بیشتر در جامعه استفاده کردند. شناخت حق و مسئولیت‌ها که در قالب آموزش‌های شهروندی ارائه می‌شود، راهی مؤثر برای پیشگیری از جرائم و آگاهی‌رسانی به شهروندان برای حفاظت از خود است. همچنین آموزش شهروندی می‌آموزد که در برخورد با مواردی که امنیت آن‌ها را به خطر می‌اندازد، چگونه رفتار کنند و به کجا مراجعه کنند. با آگاهی شهروندان و گزارش زودهنگام موارد مشکوک و جرائم سایبری، کار پلیس فتا در شناسایی و پیگیری جرائم آسان‌تر شده و احتمال

1. Sari

درگیری ناخواستهٔ افراد جامعه در چنین جرائمی کاهش می‌یابد و پیشگیری با قدرت و بهتر انجام می‌شود.

محدودیت‌ها

مهم‌ترین محدودیت این پژوهش مرور نظری موضوع بوده و به‌صورت میدانی اثربخشی آموزش شهروندی بر افزایش امنیت اجتماعی بررسی نشد.

به‌دلیل گسترده بودن بحث امنیت در این مطالعه، تمرکز بر امنیت در حوزهٔ رسانه و دیجیتال قرار داشت و به ابعاد توسعهٔ پایدار، اکولوژیک، اقتصادی، فرهنگی کمتر توجه شد.

پیشنهادها

پیشنهاد می‌شود به‌صورت پژوهش میدانی اثربخشی آموزش شهروندی بر بهبود رفتارهای مرتبط با حوزهٔ امنیت بررسی شود. در این راستا پیشنهاد می‌شود آموزش شهروندی در مقطع زمانی مشخصی برای همهٔ افراد جامعه اجباری شده و برای شرکت در این دوره آموزشی گواهی‌هایی در نظر گرفته شود. می‌توان یکی از شرایط استخدامی و یا حتی دریافت مدرک دیپلم را گذراندن چنین آموزش‌هایی در نظر گرفت و یا حتی به‌عنوان واحد درسی دانشگاهی مد نظر قرار داد.

پیشنهاد می‌شود پژوهش‌هایی برای بررسی اثربخشی همکاری نهاد آموزشی و امنیتی در پیشگیری و کاهش جرائم انجام شود.

پیشنهاد می‌شود برای تربیت افرادی که از بازنمایی در سامانه‌ها آگاه بوده، بتوانند آنچه را در رسانه ارائه می‌شود، به‌خوبی ارزیابی کرده و برای مشارکت در این عرصه دانش کافی داشته باشند، از آموزش شهروندی استفاده شود.

منابع

احمدی، ی. و مرادی، س. (۱۳۹۷). سرمایه اجتماعی (آنلاین و آفلاین) و فرهنگ شهروندی. *فصلنامهٔ علوم اجتماعی*، ۲۷ (۸۱): ۱۰۱-۱۳۳. https://doi.org/10.22054/qjss.2017.23871.1600

امیری، سروش، احدنژاد، علیرضا (۱۳۹۷). جایگاه آموزش حقوق شهروندی بر کاهش خشونت پلیس. *فصلنامه سیاست*، ۵(۱۸): ۳۵-۵۶. http://ensani.ir/file/download/article/1550387509-10070-18-3.pdf

امیریان‌فارسانی، امین، مالمیر، محمود، اشرافی، محمود، حیدری، مسعود (۱۳۹۶). کارکردهای نظری و عملی پلیس فتا در پیشگیری از جرائم سایبری و موانع حاکم بر آن. تحقیقات حقوقی تطبیقی ایران و بین‌الملل، ۱۱(۳۵): ۲۳۷-۲۶۵. article_667025_5aca88b9247f87434951af319573f7b5.pdf

بابایی، م. (۱۴۰۰، ۱۰ اسفند). بیشترین جرائم سایبری در تهران چیست؟ ایسنا. برگرفته از: https://www.isna.ir/news.

رمضانی، ر. و موحدی‌صفت، م.ر. (۱۴۰۰). رتبه‌بندی تهدیدهای اینترنت اشیاء در محیط نظامی. *فصلنامه علمی امنیت ملی*، *۱۱*(۳۹): ۱۹۹- ۲۲۸. https://journals.sndu.ac.ir/article_1396.html

سیف‌درخشنده س، عطادخت ا، حاجلو ن، میکاییلی ن. ۱۴۰۰. مدل‌یابی گرایش دانش‌آموزان به فضای مجازی بر مبنای عوامل فردی، زمینه‌ای و محیطی: ارزیابی پیامدهای روان‌شناختی آن. *مجله مطالعات روان‌شناسی تربیتی*، ۱۸(۴۴): ۱۳۵-۱۵۳.

عشایری، ط.، قنبری‌برزیان، ع.، نامیان، ف. و مهتری‌آرانی. (۱۴۰۰). بررسی تأثیر مصرف رسانه‌های جمعی بر امنیت اجتماعی شهروندان. *فصلنامه علمی امنیت ملی*، *۱۱*(۳۹): ۲۲۱- ۲۴۴. 20.1001.1.33292538.1400.11.39.11.5

فیروزی، م.ح.، موحدی‌صفت، م.ر.، ملامیرزایی، ح.ح. و موسویان، م. (۱۴۰۰). مدل مفهومی تجزیه و تحلیل کلان داده‌های رسانه‌های اجتماعی با رویکرد علوم شناختی. *فصلنامه علمی امنیت ملی*، *۱۱*(۴۱): ۱۸۷- ۲۱۸. 20.1001.1.33292538.1400.11.41.7.5

کردعلیوند، ر. و میرزایی، م. (۱۳۹۷). گونه شناسی جرائم سایبری با نگاهی به قانون جرائم رایانه‌ای و آمار پلیس فتا. *مجله حقوقی دادگستری*، *۸۲*(۱۰۲): ۱۹۱- ۲۰۷. 10.22106/JLJ.2018.32738

گل‌بهاری، ن. و رجبلو، ع. (۱۳۹۹). بررسی آموزش شهروندی در کتب درسی تعلیمات اجتماعی مقاطع سوم تا نهم با تأکید بر ساختار جدید آموزشی ۳-۳-۶. *جامعه‌شناسی نهادهای اجتماعی*، ۷(۱۵): ۳۲۴-۲۹۷. https://www.sid.ir/paper/375734/fa

متقی، ا.، داودی، م. (۱۴۰۰). درآمدی بر امنیت انرژی، امنیت ملی و حقوق شهروندی (مطالعه موردی ایران). *مطالعات حقوق انرژی*، *۷*(۱): ۲۱۱-۲۲۷. 10.22059/jrels.2021.292332.323

محمدی خانقاهی، م. و آزادی، م.ح. (۱۴۰۰). تفاوت‌های امنیت سایبری اجتماعی با امنیت سایبری. *فصلنامه علمی امنیت ملی*، *۱۱*(۳۹): ۱۳۱- ۱۵۸. https://journals.sndu.ac.ir/article_1587.html

مشکین، س.، امیدی، ج. و کردعلیوند، ر. (۱۴۰۰). کشف جرائم شرکت‌های تجاری در عرصه تولید و عرضه کالا و خدمات علیه مصرف‌کننده؛ چالش‌ها و راهکارها. *مطالعات حقوق کیفری و جرم‌شناسی*، ۵۱(۲): ۵۲۳- ۵۴۱.

هادی‌سیفی، فرزاد، احمدی‌پور، زهرا، حافظنیا، محمدرضا، مرادیان، محسن (۱۳۹۸). طراحی مدل ساختاری-تفسیری (ISM) عوامل مؤثر بر ایجاد امنیت پایدار شهروندی. *فصلنامه شهر پایدار*، ۲ (۳): ۱۱۱-۱۲۵.

Adetoro, 'N. and Okike, B., (2022). Assessing Undergraduates Social competence on Social Media in Nigeria. *Library Philosophy and Practice (e-journal).* 6788. https://digitalcommons.unl.edu/libphilprac/6788

Andreouli, E., and Brice, E. (2022). Citizenship under COVID-19: An analysis of UK political rhetoric during the first wave of the 2020 pandemic. *J Community Appl Soc Psychol, 32*:555–572.

Aslan, O. & Samet, R. (2020). A Comprehensive Review on Malware Detection Approaches. Digital Object Identifier, 8. Retrieved from: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8949524

Biswas, B. B., & Murai, N. K. (2024). From Traditional Security to Human Security: A Conceptual Framework. In Human Security in Asia: Interrogating State, Society, and Policy (pp. 57-71). Singapore: Springer Nature Singapore.

Broom, C. A. (2020). Citizenship and Social Studies Curricula in British Columbia, Canada: Contemporary Realities and Alternative Possibilities. In E. Delgado-Algarra, & J. Cuenca-López (Eds.), *Handbook of Research on Citizenship and Heritage Education* (pp. 56-79). IGI Global. https://doi.org/10.4018/978-1-7998-1978-3.ch004

Cambridge (2022). security from the Cambridge Business English Dictionary. Cambridge University Press. https://dictionary.cambridge.org/dictionary/english/security

Cann, A. (2024). Improving Citizen Security Education and Awareness in West Africa. Journal of Central and Eastern European African Studies, 3(1), 209-233.

Cao, B. (2018, Mar-Feb). Defining Environmental Citizenship. *1st European Joint Meeting*, 28 Feb-2 Mar 2018, Lemessos, Cyprus. https://enec-cost.eu/wp-content/uploads/2018/06/Keynote-Presentation-by-Dr-Benito-Cao-The-University-of-Adelaide-Australia-Defining-Environmental-Citizenship.pdf

Choi, J., Kruis, E. N., and Choo, K.S. (2021). Explaining Fear of Identity Theft Victimization Using a Routine Activity Approach. *Journal of Contemporary Criminal Justice, 37*(3): 406–426. https://doi.org/10.1177/1043986221100

Christensen P S, Boyle D K, Church H S, Wakefield I R. 2018. Social Media Use and Its Impact on Relationships and Emotions. MA. Thesis. *School of Communications. Brigham Young University*. All Theses and Dissertations, 6927. Retrieved from: https://scholarsarchive.byu.edu/etd/6927

Dal Cason, D., Casini, A. & Hellemans, C. (2020). Moral Courage Fostering Bystander Intervention Against Workplace Bullying: Findings from an Exploratory Study with a Video-Vignette Procedure. *Int Journal of Bullying Prevention 2*: 53–64. https://doi.org/10.1007/s42380-020-00062-7

Emerson, R. G. (2020). Who is the Citizen in Citizen Security? *Latin American Research Review, 55*(3): 529-543. DOI: https://doi.org/10.25222/larr.454

Goni, O. (2022). Introduction to Cyber Crime. *International Journal of Engineering and Artificial Intelligence, 3*(1): 9–23.

Grammon, A. T. (2020). *Comparing Digital Citizenship Perceptions of Online Students and Teachers*. PhD Dissertation. Liberty University. 130 p. https://digitalcommons.liberty.edu/cgi/viewcontent.cgi?article=3815&context=doctoral

Hadjichambis, Ch. A., and Hadjichambi. P. D., (2020). Environmental Citizenship Questionnaire (ECQ): The Development and Validation of an Evaluation Instrument for Secondary School Students. *Sustainability* 12(3): 821. https://doi.org/10.3390/su12030821

Harrison, T. & Polizzi, G. (2022). (In)civility and adolescents' moral decision making online: drawing on moral theory to advance digital citizenship education. *Education and Information Technologies, 27*: 3277–3297. https://doi.org/10.1007/s10639-021-10710-0

Hennell, K., Limmer, M., & Piacentini, M, (2019). Ethical Dilemmas Using Social Media in Qualitative Social Research: A Case Study of Online Participant Observation. *Sociological Research Online, 25*(3): 473–489.

Hoskins, B., Villalba, G. E., Van Nijlen, D., Barber, C. (2008). *Measuring Civic Competence in Europe: A Composite Indicator Based on IEA Civic Education Study 1999 for 14 Years Old in School.* EUR 23210 EN. Luxembourg (Luxembourg). https://doi.org/10.1002/casp.2526

James, C., Weinstein, E., & Mendoza, K. (2021). *Teaching digital citizens in today's world: Research and insights behind the Common Sense K–12 Digital Citizenship Curriculum.* (Version 2). San Francisco, CA: Common Sense Media. https://www.commonsense.org/system/files/pdf/2021-08/common-sense-education-digital-citizenship-research-backgrounder.pdf

Jones, M. L. & Mitchell, J. K. (2015). Defining and measuring youth digital citizenship. *New media & society*, 1-17. https://doi.org/10.1177/1461444815577797

Karim, A., Azam, A., Ahanmugam, B., Kannoorpatti, K., & Alazab, M. (2019). A Comprehensive Survey for Intelligent Spam Email Detection. Digital Object Identifier, 7. Retrieved from: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8907831

Keating, A. (2016). Educating Tomorrow's Citizens: What Role Can Schools Play? *Foro de Educación*, 14(20), 35-47. 10.14516/fde.2016.014.020.004

Lenhart, A., Ybarra, M., Zickuhr, K. & Price-Feeney, M. (2016). *Online Harassment, Digital Abues, and Cyberstalking in America*. Data & Society Research Institute. New York. PP: 59. https://www.datasociety.net/pubs/oh/Online_Harassment_2016.pdf

Lewis, D. and Castellino, J. (2013). Establishing a Different Dimension of Citizen Security: The Case for Special Protection for Whistleblowers. Beijing Law Review, 4(4): 185-197. http://dx.doi.org/10.4236/blr.2013.44024

Mahadir, B. N., Baharudin, H. N., and Ibrahim, N. N. (2021). Digital citizenship skills among undergraduate students in Malaysia: A preliminary study. International Journal of Evaluation and Research in Education, 10(3): 835-544. DOI: 10.11591/ijere.v10i3.21277

Maher, C. A. (2024). Examining the Association Between Citizenship and Ethnicity on Identity Theft Risk: Findings from the National Crime Victimization Survey. *American Journal of Criminal Justice*, 1-22.

Malinauskas, R. & Malinauskiene, V. (2019). A meta-analysis of psychological interventions for Internet/smartphone addiction among adolescents. *Journal of Behavioral Addictions, 8*(4): 613–624. DOI: 10.1556/2006.8.2019.72

Nieuwelink, H. & Oostdam, R. (2021): Time for citizenship in teacher training. *Journal of Social Science Education* 20 (3): 130-146. https://doi.org/10.11576/jsse-4030

Ortiz, M. S. (2020). Trolling as a Collective Form of Harassment: An Inductive Study of How Online Users Understand Trolling. *Social Media + Society*. 1-9. Retrieved from: journals.sagepub.com/home/DOI: 10.1177/2056305120928512

Padín, P. F., González-Rodríguez, R., Verde-Diego, C., & Vázquez-Pérez, R. (2021). Social media and eating disorder psychopathology: A systematic review. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 15(3), Article 6. https://doi.org/10.5817/CP2021-3-6.

Putu Anggie, I.A. S., & Ipnuwati, S. (2022). Ethics of Internet Use (Digital Netiquette) in UU ITE Perspective: Building a Courteous Digital Culture in the Era of Digital Transformation. Journal of Image Processing and Intelligent Remote Sensing, 2(4): 8-14. https://doi.org/10.55529/jipirs.24.8.14

Rejekiningsih, T. (2015). Law Awareness Forming Strategies to Reinforce the Principles of Social Function of Land Rights Within the Moral Dimension of Citizenship. 2nd *Gloal Conference on Business and Social Science*, 17-18 September, Bali, Indonesia. 10.1016/j.sbspro.2015.11.011

Richardson, J. & Milovidov, E. (2019). *Digital Citizenship Education Handbook.* Concil of Europe Publishing. Strasbourg, Cedex.144 P. https://rm.coe.int/16809382f9

Richardson, J., Milovidov, E., and Schmalzried, M. (2017). *Internet literacy handbook*. Council of Europe. Concil of Europe Publishing. Strasbourg, Cedex. 147 P. https://edoc.coe.int/en/internet/7515-internet-literacy-handbook.html

Sari, I. D., Rejekiningsih, T. Muchtarom, M. (2020). Students' Digital Ethics Profile in the Era of Disruption: An Overview from the Internet Use at Risk in Surakarta City, Indonesia. *IJIM, 14*(3): 82-93. https://doi.org/10.3991/ijim.v14i03.12207

Satidporn, W. (2022). *Citizen Participation in Thai Politics: A Critical Review. Democracy x Innovations Working Paper Series*, no. 3. Bangkok: King Prajadhipok's Institute. Satidporn, Wichuda, Citizen Participation in Thai Politics: A Critical Review (March 9, 2022). Available at SSRN: https://ssrn.com/abstract=4053206 or http://dx.doi.org/10.2139/ssrn.4053206

Sedgwick, R., Epstein, S., Dutta, R. and Ougrin, D. (2019). Social media/internet use and suicide attempts. *Child and adolescent psychiatry, 32*(6): 534-541. doi: 10.1097/YCO.0000000000000547

Sinthiya, A. P. A. I. & Ipnuwati, S. (2022). Ethics of Internet Use (Digital Netiquette) in UU ITE Perspective: Building a Courteous Digital Culture in the Era of Digital Transformation. *Journal of Image Processing and Intelligent Remote Sensing, 2*(4): 8-14. https://doi.org/10.55529/jipirs.24.8.14

Sun, Z., Oest, A., Zhang, P., Rubio-Medrano, C., Bao, T., Wang, R., Zhao, Z., Shoshitaishvili, Y. Doupé, A., & Ahn, G.J. (2021). Having Your Cake and Eating It: An Analysis of Concession-Abuse-as-a-Service. *30th USENIX Security Symposium*. (August 11–13). Anaheim, CA, United States. https://www.usenix.org/system/files/sec21-sun-zhibo.pdf

T. K. H. Chan, H. K. T., Christy M. K. Cheung, K. M. C., Benbasat, I., Xiao, B., Lee, Y. W. Z. (2022). Bystanders Join in Cyberbullying on Social Networking Sites: *The Deindividuation and Moral Disengagement Perspectives*: 23-16. Retrieved from: https://pubsonline.informs.org/doi/10.1287/isre.2022.1161.

Telešienė, A., Pauw, B. J., Goldman, D. and Hansmann, R. (2021). Evaluating an Educational Intervention Designed to Foster Environmental Citizenship among Undergraduate University Students. *Sustainability* 13(15): 8219. https://doi.org/10.3390/su13158219

Wong, Y. H., Mo, Y. H., Potenza, N., M., Chan, N.M. M., Lau, M. W., Chui, K. T., Pakpour, H. A., and Lin, C. (2020). Relationships between Severity of Internet Gaming Disorder, Severity of Problematic Social Media Use, Sleep Quality and Psychological Distress. *International Journal of Environmental Research and Public Health, 17*: 1879-1892. https://doi.org/10.3390/ijerph17061879

Xu, J., Xu, X., & Jia, G. (2024). Resource efficiency, green development, and social security: Evidence from ASEAN+ 6 economies. Resources Policy, 90, 104744.

Zulqadri, M. D., Mustadi, A., & Retnawati, H. (2022). Digital Safety Online Learning: What We Do to Protect Our Students? *Jurnal Iqra': Kajian Ilmu Pendidikan, 7*(1): 178-191. https://doi.org/10.25217/ji.v7i1.1746

Modern citizenship Education and security (necessities and functions)

Elham Irannezhad,[1*] Ali Mahdad,[2] Mohsen Golparar[3]

Received: 03/12/2023 Accepted: 12/03/2024

Abstract

Nowadays, more than half of the world's population lives in cities and considering that cities have problems and crises in different dimensions that affect security, the link between Citizenship and security have increased. Therefore, security has been turned from the traditional form: finance and trade, bank accounts and transactions to the new dimensions of sustainable development, environment, media and digital, and even for its new dimensions, the specialized police of FATA (Cyber-police) was created with the aim of securing cyber space, maintaining security and legitimate freedoms of citizens and protecting the infrastructure of the country against cyber attacks and crimes, and was formed. Knowing the rights and responsibilities that are presented in the form of citizenship education is an effective way to prevent crimes and inform citizens to protect themselves. Also, citizenship education teaches how to behave and where to go when dealing with things that endanger their security. With citizens' awareness and early reporting of suspicious cases and cyber-crimes, the work of FATA police in identifying and following up on crimes becomes easier and the possibility of unwanted involvement of people in such crimes is reduced and prevention is done better and stronger.

Keywords: citizenship, security, virtual space, FATA police.

1. PhD Student, Department of psychology, Isfahan (Khorasgan) Branch, Islamic Azad University, Isfahan, Iran, (Corresponding Author); elhamirannegad@yahoo.com
2. Associate Professor, Department of psychology, Isfahan (Khorasgan) Branch, Islamic Azad University, Isfahan, Iran; alimahdad.am@gmail.com
3. Professor, Department of psychology, Isfahan (Khorasgan) Branch, Islamic Azad University, Isfahan, Iran; drmgolparvar@hotmail.com
Doi: 10.22052/IJCS.2024.253891.1023