JURNAL PENGABDIAN MASYARAKAT BANGSA
e-ISSN : 2987- 0135
Volume 3, No. 5, Tahun 2025
https://jurnalpengabdianmasyarakatbangsa.com/index.php/jpmba/index

Pelatihan Memahami Jejak Digital dan Doxing: Kesadaran dan Strategi Literasi

Dedi Kurnia Syah Putra[1], Hadi Purnama[2], Sri Wahyuning Astuti[3], Sang Ayu Putu Vajravany Yudyaputri Warasenda[4]
[1,2,3,4] *Universitas Telkom, Indonesia*

Corresponding Author
Nama Penulis: Sri Wahyuning Astuti
E-mail: sriwahyuning@telkomuniversity.ac.id

Abstrak

Siswa SMA merupakan kelompok yang sangat rentan terhadap berbagai ancaman digital, termasuk doxing. Remaja cenderung kurang memahami batasan privasi dalam dunia digital, sehingga sering kali membagikan informasi pribadi tanpa menyadari potensi risikonya. Ketidaktahuan ini membuat mereka lebih mudah menjadi target eksploitasi data pribadi. Fenomena doxing menyebabkan efek psikologis yang mendalam, seperti kecemasan, stres, dan gangguan mental lainnya. Siswa yang mengalami doxing dapat mengalami ketakutan dalam berinteraksi secara online, yang berdampak pada kehidupan sosial dan akademik mereka. Dalam beberapa kasus, doxing bahkan dapat menyebabkan cyberbullying yang lebih luas dan berujung pada depresi atau tindakan yang lebih ekstrem. Edukasi tentang bahaya doxing dan cara melindungi informasi pribadi harus menjadi bagian dari kurikulum literasi digital di sekolah. Pelatihan terkait Jejak Digital dan Doxing: Risiko dan Pencegahannya dilakukan kepada siswa siswi MAN 1 Pangandaran, dengan memberikan pemahaman terkait penggunaan media sosial, mengelola penggunaan dan jejak digital yang kemungkinan muncul dari penggunaan media sosial. Siswa Juga perlu diberikan pemahaman antisipasi doxing dan Langkah yang perlu dilakukan jika mengalami doxing di media sosial. Hasil Kegiatan berupa peningkatan pengetahuan terkait jejak digital dan doxing, serta kemampuan untuk mencegah dan mengatasi dampak doxing.
Kata Kunci - *doxing, literasi digital. over sharing, cybercrime*

Abstract

High school students are a group that is particularly vulnerable to various digital threats, including doxing. Teenagers tend to lack understanding of the limits of privacy in the digital world, so they often share personal information without realizing the potential risks. This ignorance makes it easier for them to become targets for personal data exploitation. The phenomenon of doxing causes profound psychological effects, such as anxiety, stress, and other mental disorders. Students who experience doxing can experience fear in interacting online, which impacts their social and academic lives. In some cases, doxing can even lead to more widespread cyberbullying and lead to depression or more extreme actions. Education about the dangers of doxing and how to protect personal information should be part of the digital literacy curriculum in schools. Training related to Digital Footprint and Doxing: Risks and Prevention was carried out to MAN 1 Pangandaran students, by providing an understanding of the use of social media, managing the use and digital footprint that may arise from the use of social media. Students also need to be given an understanding of doxing anticipation and the steps that need to be taken if they experience doxing on social media. The results of the activity are in the form of increased knowledge regarding digital footprints and doxing, as well as the ability to prevent and overcome the impacts of doxing.
Keywords *- doxing, digital literacy. over sharing, cybercrime*

PENDAHULUAN

Tahun 2024 ini diperkirakan sekitar 221.563.000 orang dari total populasi 288 juta sudah terkoneksi internet atau mencapai tingkat penetrasi sekitar 79,5 persen. Angka ini meningkat sekitar 1,4 persen dari tahun 2023. Dari jumlah itu, urutan Pertama penggunaan adalah generasi milenial, yakni mereka yang lahir pada 1981 sampai 1996 menyumbang pengguna internet tertinggi, yaitu sekitar 93,17 persen dengan kontribusi sekitar 30,6 persen dari total pengguna internet di Indonesia. Posisi tertinggi kedua adalah Generasi Z (Gen Z) atau kelahiran 1997-2002 sekitar 87,2 persen dengan kontribusi hingga 34 persen dari total pengguna internet di Indonesia. Kemudian Generasi X yang lahir pada 1965-1980 sekitar 83,69 persen dengan kontribusi sekitar 18,90 persen dan total pengguna internet di Indonesia.

Sejumlah kasus terkait banyaknya penyalahgunaan penggunaan media sosial banyak dilaporkan media, mulai dari penipuan menggunakan akun palsu hingga hate speech. Dalam beberapa tahun terakhir bahkan kejahatan yang melibatkan dunia maya semakin meningkat dari hari kehari mulai dari mereka pengguna media sosial dengan akun nyata hingga akun anonim.

Data dari kementrian komunikasi menyebutkan, banyak data pribadi disalahgunakan dengan modus operandi menggunakan fitur aplikasi, diantaranya penggunaan aplikasi fitur stiker Add Yours di Instagram Stories. Fitur pada isntagram ini menjadi celah kejahatan dengan modus teknik social engeenering. Social engineering sendiri adalah teknik manipulasi psikologi agar individu atau grup mau melakukan sesuatu atau menyerahkan informasi tertentu secara sukarela.Kejahatan di dunia maya dengan memanfaatkan faktor psikologis pengguna internet terus meningkat dengan beragam teknik, diantaranya dengan melakukan catfishing (Audinia et al., 2023)

Siswa SMA merupakan kelompok yang sangat rentan terhadap berbagai ancaman digital, termasuk doxing. Menurut penelitian yang dilakukan oleh Marwick dan boyd (2018), remaja cenderung kurang memahami batasan privasi dalam dunia digital, sehingga sering kali membagikan informasi pribadi tanpa menyadari potensi risikonya. Ketidaktahuan ini membuat mereka lebih mudah menjadi target eksploitasi data pribadi oleh pihak yang tidak bertanggung jawab. Oleh karena itu, edukasi tentang bahaya doxing dan cara melindungi informasi pribadi harus menjadi bagian dari kurikulum literasi digital di sekolah (Marwick & boyd, 2018)

Fenomena doxing tidak hanya berdampak pada individu yang menjadi korban, tetapi juga dapat menyebabkan efek psikologis yang mendalam, seperti kecemasan, stres, dan gangguan mental lainnya (Hinduja & Patchin, 2019). Siswa yang mengalami doxing dapat mengalami ketakutan dalam berinteraksi secara online, yang berdampak pada kehidupan sosial dan akademik mereka. Dalam beberapa kasus, doxing bahkan dapat menyebabkan cyberbullying yang lebih luas dan berujung pada depresi atau tindakan yang lebih ekstrem. Oleh karena itu, pemahaman tentang etika digital dan pentingnya menjaga privasi harus diajarkan secara sistematis (Patchin & Ph, 2019)

Selain aspek perlindungan diri, edukasi tentang literasi doxing juga penting untuk mencegah siswa menjadi pelaku. Banyak kasus doxing yang terjadi di kalangan remaja diawali dari keisengan atau keinginan untuk membalas dendam tanpa memahami konsekuensinya (Citron, 2014). Dengan pemahaman yang baik mengenai dampak hukum dan sosial dari tindakan doxing, siswa diharapkan dapat lebih bijak dalam menggunakan media digital dan tidak terlibat dalam aktivitas yang dapat merugikan orang lain (Citron, 2014)

Pentingnya literasi digital telah ditekankan oleh berbagai lembaga pendidikan dan organisasi internasional. UNESCO (2021) menyoroti bahwa literasi digital harus mencakup pemahaman tentang privasi, keamanan data, serta etika dalam berinteraksi di dunia maya. Sayangnya, di Indonesia, pembelajaran mengenai literasi digital, khususnya yang terkait dengan risiko doxing, masih belum menjadi perhatian utama dalam kurikulum sekolah. Padahal, dengan meningkatnya jumlah pengguna internet di kalangan remaja, kebutuhan akan edukasi ini menjadi semakin mendesak (UNESCO., 2021)

Sebagai bagian dari upaya mitigasi risiko doxing, sekolah dapat berperan aktif dengan mengintegrasikan program literasi digital dalam pembelajaran sehari-hari. Beberapa langkah yang

dapat dilakukan meliputi pelatihan tentang pengelolaan data pribadi, simulasi kasus doxing dan cara mengatasinya, serta sosialisasi mengenai regulasi perlindungan data pribadi (Livingstone et al., 2017). Dengan demikian, siswa tidak hanya memahami bahaya doxing, tetapi juga memiliki keterampilan untuk mencegah dan menanggapi ancaman tersebut secara efektif (Livingstone, S., Davidson, J., Bryce, J., Batool, S., Haughton, C., & Nandi, 2019)

Peran orang tua juga tidak kalah penting dalam mendukung literasi digital anak. Studi menunjukkan bahwa keterlibatan orang tua dalam mendidik anak-anak mereka tentang keamanan digital dapat mengurangi risiko mereka menjadi korban kejahatan siber (Livingstone & Helsper, 2007). Oleh karena itu, program literasi digital di sekolah sebaiknya melibatkan orang tua agar edukasi yang diberikan lebih komprehensif dan efektif (Livingstone & Helsper, 2007)

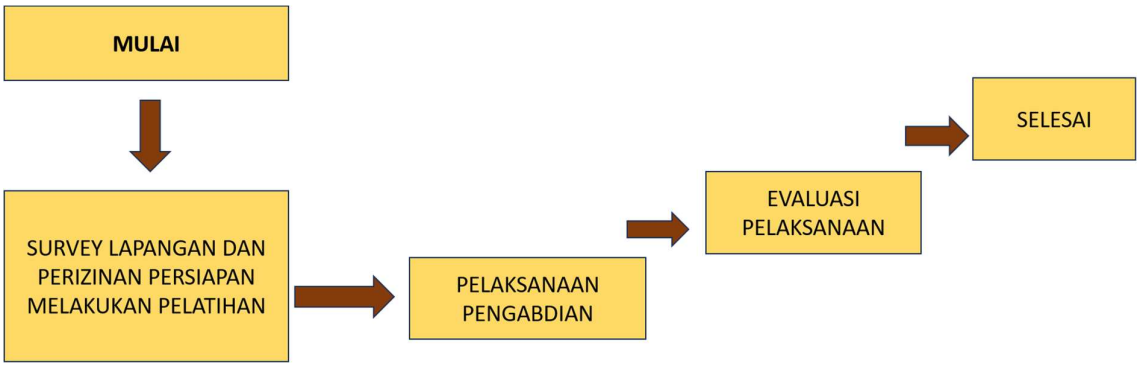
Selain itu, pemerintah dan lembaga terkait perlu berperan aktif dalam menyediakan regulasi dan kebijakan yang melindungi anak-anak dari ancaman digital. Undang-Undang Perlindungan Data Pribadi yang sedang dikembangkan di Indonesia diharapkan dapat memberikan perlindungan lebih bagi pengguna internet, termasuk siswa SMA (Kementerian Komunikasi dan Informatika, 2022). Namun, regulasi saja tidak cukup; diperlukan upaya kolaboratif antara sekolah, orang tua, dan masyarakat untuk meningkatkan kesadaran akan pentingnya keamanan digital.

Dengan adanya literasi doxing yang baik, siswa SMA dapat lebih memahami bagaimana menjaga informasi pribadi mereka, menghindari ancaman doxing, serta menggunakan internet dengan lebih bijak dan bertanggung jawab. Kesadaran ini tidak hanya akan melindungi mereka dari risiko digital, tetapi juga membentuk generasi yang lebih sadar akan etika dan keamanan dalam dunia maya.

METODE

Metode Pelaksanaan Pengabdian Pada Masyarakat dimulai dari

1. Survey lapangan dan perizinan ke tempat pengabdian masyarakat Survey dilakukan setelah proposal rencana kegiatan di setujui oleh pihak kampus. Survey dilakukan beberapa kali untuk memastikan kesiapan waktu dan lokasi serta sarana dan prasarana yang dibutuhkan saat pelaksanaan abdimas.
2. Melakukan persiapan ke lokasi. Persiapan dilakukan dengan memastikan ruangan yang digunakan, seperti kesiapan proyektor, mic, speaker dan alat alat lain yang dibutuhkan untuk kepentingan praktek maupun teori.
3. Membuat materi tentang "Komunikasi Digital" yang meliputi
   a) 1.Jejak Digital
   b) 2.Fenomena Doxing
   c) 3. Pencegahan Doxing
4. Tahapan selanjutnya adalah pelaksanaan kegiatan dengan sebelumnya dilakukan pretest.
5. Pelaksanaan kegiatan diawali dengan memberikan pretest yakni sejumlah pertanyaan terkait beberapa materi terkait keamanan data digital. Hasil pretes akan menjadi pembanding dengan hasil post test atau setelah materi diberikan
6. Pelaksanaan ceramah dilakukan dengan memberikan materi dan tanya jawab kepada peserta.
7. Setelah pemberian materi selesai dilakukan maka diberikan post tes dilanjutkan dengan evaluasi pelaksanaan. Proses Evaluasi berupa rangkaian kegiatan dari awal hingga akhir.
8. Post test diberikan setelah rangkaian pemberian materi, untuk mengetahui tingkat keterserapan materi yang diberikan. Soal Post Test memiliki pertanyaan yang sama dengan pre test. Peserta juga diberikan pertanyaan evaluasi untuk mengetahui penilaian peserta atas seluruh rangkaian kegiatan.
9. Berdasarkan hasil pre test dan post tes, untuk selanjutnya dilakukan kesimpulan terhadap kegiatan pengabdian masyarakat ini dan rencana keberlanjutan berdasarkan hasil feed back dari peserta.



Gambar 1.
Alur Kegiatan Pengabdian

HASIL DAN PEMBAHASAN

Pemberian Materi terkait Jejak Digital dan Doxing dilakukan dengan menggunakan ceramah pada sekitar 30 Siswa dan Siswi MAN 1 Pangandaran. Peserta yang merupakan siswa dan siswi aktif dan duduk di kelas kelas XI, diberikan materi terkait jejak digital, etika posting, doxing, dan Langkah untuk menghindari dan mengatasi doxing.

Pemahaman terkait Jejak digital dimulai dengan memberikan Penjelasan terkait pengertian Jejak digital (digital footprint). Jejak Digital adalah rekam data yang tertinggal setelah seseorang melakukan aktivitas di dunia maya. Setiap interaksi digital—seperti mengakses situs, mengunggah konten, atau menggunakan aplikasi—meninggalkan jejak berupa data. Menurut (Solove, 2004) data ini dapat dikumpulkan, disimpan, dianalisis, dan disebarluaskan oleh berbagai pihak, termasuk platform digital dan pengiklan. Fenomena ini menuntut pengguna untuk lebih sadar terhadap konsekuensi dari perilaku digital mereka.

Jejak digital terbagi menjadi dua bentuk utama: jejak aktif dan jejak pasif. Jejak aktif muncul ketika individu secara sadar membagikan informasi, seperti membuat status media sosial atau mengisi formulir daring. Sebaliknya, jejak pasif terbentuk tanpa interaksi langsung, misalnya melalui cookie, pelacakan IP address, dan data lokasi (Tufekci, 2014). Dengan berkembangnya teknologi pelacakan dan big data, kedua bentuk jejak ini dapat dipadukan untuk membentuk profil pengguna yang sangat rinci.

Gambar 2.
Pemateri Jejak Digital

Dampak dari jejak digital bersifat ambivalen. Di satu sisi, ia dapat dimanfaatkan untuk membangun reputasi profesional dan personal branding, seperti portofolio daring atau kontribusi

akademik. Namun di sisi lain, jejak digital juga menyimpan potensi risiko serius, seperti pelanggaran privasi, pencurian identitas, dan cyberbullying (Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, 2009). Bahkan, data digital yang terkumpul dapat dimanfaatkan untuk profiling dan manipulasi perilaku oleh algoritma, sebagaimana ditunjukkan dalam kasus Cambridge Analytica.

Mengelola jejak digital memerlukan literasi digital yang kuat. Beberapa langkah yang direkomendasikan antara lain: mengaktifkan pengaturan privasi, menggunakan autentikasi dua faktor, tidak sembarangan memberikan izin aplikasi, serta secara berkala membersihkan riwayat aktivitas digital (Livingstone & Helsper, 2007) Institusi pendidikan dan organisasi juga disarankan menerapkan kebijakan keamanan siber dan memberi pelatihan kepada anggotanya untuk memperkuat kesadaran dan tanggung jawab digital.

Jejak digital dan doxing memiliki keterkaitan yang erat karena doxing memanfaatkan jejak digital sebagai sumber utama informasi. Doxing (atau doxxing) adalah tindakan mengumpulkan dan menyebarkan informasi pribadi seseorang secara daring tanpa izin, biasanya dengan maksud merugikan, mempermalukan, atau mengancam target (Douglas, 2016). Informasi tersebut—seperti alamat rumah, nomor telepon, identitas keluarga, hingga data pekerjaan—sering kali diperoleh dari jejak digital yang ditinggalkan oleh individu secara sadar (jejak aktif) maupun tanpa sadar (jejak pasif). Artinya, semakin banyak dan terbukanya informasi yang tersedia di internet, semakin besar peluang seseorang menjadi korban doxing.

Fenomena ini menjadi semakin mengkhawatirkan karena banyak orang tidak menyadari sejauh mana data mereka tersebar dan tersimpan secara publik. Studi oleh (Solove, 2007) menekankan bahwa pengumpulan data personal di era digital memiliki konsekuensi serius terhadap privasi dan keamanan individu. Dalam konteks ini, jejak digital yang tidak dikelola dengan baik dapat menjadi senjata bagi pelaku doxing untuk menyerang korban secara psikologis, sosial, bahkan hukum. Oleh karena itu, penting bagi pengguna internet untuk menerapkan prinsip hygiene digital, seperti membatasi informasi pribadi yang dibagikan di platform terbuka dan secara rutin mengevaluasi jejak digital mereka di berbagai layanan daring.

Gambar 3.
Pemateri

Doxing adalah tindakan mengungkap dan menyebarluaskan informasi pribadi seseorang secara daring tanpa persetujuan, biasanya dengan niat jahat. Ciri utama dari doxing adalah penggunaan data pribadi seperti nama lengkap, alamat rumah, nomor telepon, foto keluarga, informasi tempat kerja, hingga riwayat akun media sosial, yang diambil dari berbagai sumber daring tanpa sepengetahuan korban (Douglas, 2016) Doxing dapat bersifat langsung (misalnya menyebarkan identitas korban dalam forum publik) atau terselubung, seperti menggabungkan potongan-potongan informasi dari jejak digital untuk membentuk profil menyeluruh seseorang (Solove, 2007)

Karakteristik doxing mencakup unsur intensionalitas, publikasi informasi personal tanpa izin, dan niat untuk merugikan. Pelaku doxing kerap memanfaatkan media sosial, forum diskusi, situs gelap, atau mesin pencari arsip data untuk mengumpulkan informasi korban (Mills, 2017). Target doxing bisa siapa saja—jurnalis, aktivis, akademisi, atau bahkan pelajar biasa—dan sering kali doxing terjadi sebagai bagian dari konflik daring, balas dendam digital, atau pembungkaman opini. Karakteristik lainnya adalah sifat serangan yang cepat menyebar dan sulit dikendalikan setelah informasi dipublikasikan.

Gambar 4.
Siswa MAN 1 Pangandaran

Dampak dari doxing sangat serius, termasuk tekanan psikologis, intimidasi, pelecehan daring, bahkan ancaman fisik. Dalam beberapa kasus, korban terpaksa meninggalkan rumah, kehilangan pekerjaan, atau mengalami gangguan kesehatan mental akibat teror digital (Citron, 2014). Untuk penanganan, diperlukan kombinasi langkah teknis dan hukum: mengarsip bukti penyebaran data, melaporkan ke platform digital dan pihak berwajib, serta memperkuat keamanan digital (seperti pengaturan privasi dan penghapusan data dari situs pencarian data). Edukasi literasi digital juga menjadi kunci pencegahan, terutama untuk memahami cara melindungi informasi pribadi dan mengenali potensi risiko sejak dini (Astuti et al., 2025)

Rangkaian kegiatan diakhiri dengan dilakukan evalusai terhadap pelaksanaan kegiatan, evaluasi dilakukan dengan memberikan kuesioner evaluasi, dengan hasil sebagai berikut

Tabel 1.
Kuesioner Umpan Balik Mitra

NO	Pernyataan	Sangat Setuju	Setuju	Jumlah
1	Materi kegiatan bermanfaat dan sesuai dengan kebutuhan peserta	100	0	100
2	Waktu pelaksanaan kegiatan ini relatif sesuai dan cukup	90	10	100
3	Materi yang disajikan jelas dan mudah dipahami	100	0	100
4	Tim panitia memberikan pelayanan yang baik selama kegiatan	100	0	100
5	Peserta berharap kegiatan-kegiatan seperti ini dilanjutkan di masa yang akan datang	100	0	100

Tabel diatas menunjukkan bahwa dari 30 responden yang mengikuti pelatihan, sebagian besar menyatakan sangat setuju jika kegiatan ini kembali dilakukan. Mereka juga menyatakan persetujuan atas waktu penyelenggaraan dan materi. Hasil kuesiner evaluasi dapat disimpulkan bahwa seluruh responden menginginkan kegiatan ini bisa dilanjutkan di sesi berikutnya dengan lebih banyak praktek

dan contoh (Astuti et al., 2023)

KESIMPULAN

Setelah dilakukan ceramah, diskusi dan tanya jawab pada siswa dan siswi MAN 1 Pangandaran, disimpulkan bahawa secara keseluruhan peserta mengikuti dengan antusias pemberian materi yang disampaikan mulai dari pemberian penjelasan terkait Jejak Digital dan Doxing. Peserta juga sangat antusius dalam bertanya dan mencari solusi atas permasalahan yang dihadapi generasi z dalam penggunaan fenomena jejak digital termasuk antisipasi yang bisa dilakukan untuk menghindari kejahatan yang mungkin terjadi. Untuk kedepannya kegiatan ini bisa dilakukan secara berkesinambungan, dan dijadikan kegiatan rutin sebagai bagian dari kegiatan literasi digital mengingat perkembangan teknologi selalu disertai dampak yang muncul, sehingga diperlukan pendampingan dalam penggunaannya.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada MAN 1 Pangandaran dan Semua pihak yang membantu terlaksananya pengabdian masyarakat ini.

DAFTAR PUSTAKA

Astuti, S. W., Imran, A. I., Purnama, H., & Gede, S. (2025). *Literasi Keamanan Digital Antisipasi Cat Fishing*. *2*(11), 5475–5481.

Astuti, S. W., Lestari, M. T., & Purnama, H. (2023). Pelatihan Menjadi Presenter Handal di SMK Telkom Bandung. *Jurnal Altifani Penelitian Dan Pengabdian Kepada Masyarakat*, *3*(1), 160–166. https://doi.org/10.25008/altifani.v3i1.351

Audinia, S., Maulina, D., Novrianto, R., Sudewaji, B. A., & Lotusiana, I. A. (2023). The Development of Cyberbullying in Social Media Scale. *Jurnal Pengukuran Psikologi Dan Pendidikan Indonesia*, *12*(1), 80–92. https://doi.org/10.15408/jp3i.v12i1.24142

Citron, D. K. (2014). *Hate crimes in cyberspace.* Harvard University Press.

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication, 15*(1), 83–108.

Douglas, D. M. (2016). Doxing: A conceptual analysis. *Ethics and Information Technology*, *18*(3), 199–210. https://doi.org/https://doi.org/10.1007/s10676-016-9406-0

Livingstone, S., Davidson, J., Bryce, J., Batool, S., Haughton, C., & Nandi, A. (2019). Children's Online Activities, Risks and Safety: A Literature Review by the UKCCIS Evidence Group. *UK Council for Child Internet Safety*, .

Livingstone, S., & Helsper, E. (2007). Gradations in digital inclusion: Children, young people and the digital divide. *New Media and Society*, *9*(4), 671–696. https://doi.org/10.1177/1461444807080335

Marwick, A. E., & boyd, danah. (2018). Understanding Privacy at the Margins. *International Journal of Communication*, *12*, 1157–1165. https://ijoc.org/index.php/ijoc/article/view/7053/2293%0Ahttps://ijoc.org/index.php/ijoc/article/view/7053

Mills, A. J. (2017). Protecting yourself in the age of doxing. https://doi.org/10.1016/S1361-3723(17)30066-7. *Computer Fraud & Security*, *7*(1), 14–17.

Patchin, J. W., & Ph, D. (2019). *Cyberbullying : Edition*.

Solove, D. J. (2004). *The digital person: Technology and privacy in the information age.* New York University Press.

Solove, D. J. (2007). *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet.* Yale University Press.

Tufekci, Z. (2014). Big questions for social media big data: Representativeness, validity and other methodological pitfalls. *Proceedings of the Eighth International AAAI Conference on Weblogs and Social Media.*

UNESCO. (2021). *Re|Shaping Policies for Creativity: Addressing Culture as a Global Public Good.*