JURNAL PENGABDIAN MASYARAKAT BANGSA
e-ISSN : 2987- 0135
Volume 2, No. 10, Tahun 2024
https://jurnalpengabdianmasyarakatbangsa.com/index.php/jpmba/index

Pentingnya Peningkatan Literasi Keamanan Digital Bagi Siswa SMP Negeri 4 Kota Tasikmalaya Untuk Melindungi Data Pribadi

Elsa Sapitri[1], Aulia Rahmah[2], Fathir Qisti Muhajir[3], Idah Mudrikah[4], Indriani Dewi Nurul Fajriyah[5], Najwa Nurshadrina[6], Nasfa Fitriani Syehar[7], Puput Sabriyanti Maesaroh[8], Rafi Khairi[9], Zulfa Nandiana[10], Ahmad Hamdan[11]

[1,2,3,4,5,6,7,8,9,10,11] *Universitas Siliwangi, Indonesia*

Corresponding Author
Nama Penulis: Elsa Sapitri
E-mail : elsasyapitri@gmail.com

Abstrak

Pada era digital seperti ini, penggunaan media sosial semakin tinggi sehingga resiko kebocoran data pribadi kemungkinan semakin meningkat.Perlindungan data pribadi merupakan upaya yang dilakukan seseorang untuk melindungi data pribadinya baik dalam sistem elektronik maupun nonelektronik dari ancaman kebocoran data. Lemahnya perlindungan data pribadi di indonesia mengakibatkan maraknya kebocoran data, dikarenakan kelalaian individu yang menganggap remeh terhadap data pribadi yang mereka unggah di media sosial. Isu tersebut menjadi suatu hal yang tidak terlalu penting bagi masyarakat, sehingga perlu diadakannya suatu pengabdian terkait pentingnya peningkatan literasi keamanan digital dan perlindungan data pribadi. Adapun kegiatan pengabdian ini bertujuan untuk menganalisis data pribadi baik dalam sistem elektronik maupun nonelektronik di Sekolah Menengah Pertama Negeri (SMPN) 4 Kota Tasikmalaya. Adapun metode yang digunakan pengabdian ini yaitu melalui studi pengumpulan data berupa pengabdian dan melakukan sesi kuesioner terhadap peserta didik. Hasil yang kami temukan dari kegiatan pengabdian ini yaitu bahwa siswa kurang mengetahui bagaimana cara untuk melindungi data pribadi di media sosial, mereka hanya baru mengetahui dasar dari perlindungan hp saja yaitu menggunakan pin atau kata sandi. Maka dari itu, pengabdian dilakukan dengan memberikan materi mengenai pengenalan dan juga bagaimana cara melindungi data pribadi seperti cara mengolah sandi yang benar agar tidak terjadinya kebocoran data dan cara menjaga data pribadi yang ada di website-website maupun secara langsung. Sehingga, pengabdian ini mampu meningkatkan literasi keamanan igital dan perlindungan data pribadi bagi siswa SMPN 4 Kota Tasikmalaya.

Kata kunci - *literasi digital, perlindungan data, keamanan digital*

Abstract

In this digital era, the use of social media is increasing so that the risk of personal data leakage is likely to increase. Personal data protection is an effort made by someone to protect their personal data both in electronic and non-electronic systems from the threat of data leakage. The weak protection of personal data in Indonesia has resulted in rampant data leakage, due to the negligence of individuals who underestimate the personal data they upload on social media. This issue is something that is not too important for the community, so it is necessary to hold a community service related to increasing digital security literacy and personal data protection. This community service activity aims to analyze personal data both in electronic and non-electronic systems at State Junior High School (SMPN) 4 Tasikmalaya City. The method used in this community service is through a data collection study in the form of community service and conducting a questionnaire session with students. The results we found from this community service activity were that students did not know how to protect personal data on social media, they only knew the basics of cellphone protection, namely using a pin or password. Therefore, the service is carried out by providing materials on the introduction and also how to protect personal data such as how to process the correct password to prevent data leakage and how to protect personal data on websites or directly. Thus, this service is able to increase security literacy and personal data protection for students of SMPN 4 Kota Tasikmalaya.

Keywords - digital literacy, data protection, digital security

PENDAHULUAN

Seiring berkembangnya teknologi, pendistribusian informasi dan data tentu akan semakin cepat. Kini internet sudah lebih variatif tidak hanya memiliki satu fungsi, bahkan bisa menjadi sarana untuk bertransaksi dimasa sekarang dan masa mendatang. (Kurniawan et al., 2022). Penggunaan gadget seperti *smartphone*, tab, laptop, dan komputer menjadi sarana untuk mencari informasi dan berkomunikasi. Saat ini perkembangan teknologi informasi dan internet telah mengubah cara manusia dalam berkomunikasi. Contohnya perkembangan media sosial yang sudah menjadi bagian dari kehidupan manusia untuk memperoleh, membagikan dan menyebarluaskan berbagai informasi. Media sosial adalah medium di internet yang memungkinkan pengguna merepresentasikan dirinya maupun berinteraksi, bekerja sama, berbagi, berkomunikasi dengan pengguna lain membentuk ikatan sosial secara virtual. Semakin berkembangnya media sosial maka masalah keamanan informasi dan privasi juga menjadi hal yang penting saat ini (Nasrullah, 2016 dalam Febriansyah, 2020). Maka diperlukannya sebuah pemahaman terkait pentingnya menjaga data pribadi.

Menurut Undang-Undang Nomor 27 Tahun 2022 tentang perlindungan data dribadi. Data pribadi adalah setiap data tentang kehidupan seseorang baik yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik. Saat ini media sosial sudah menjadi salah satu sumber kebocoran informasi pribadi yang sudah menjadi hal yang umum. Tanpa sadar, sudah banyak data privasi seseorang yang telah bocor di internet khususnya di media sosial. Data privasi tersebar disebabkan oleh kelalaian maupun penyedia layanan. Masyarakat memerlukan pengetahuan mengenai ancaman-ancaman yang mungkin terjadi dalam melakukan transaksi yang sering disebut dengan pengetahuan internet (*internet knowledge*) sehingga dapat mengatasi permasalahan mengenai kebocoran data pribadi. Pengetahuan terhadap internet (*internet knowledge*) dapat mengarah pada karakteristik individu yang berkembang seiring berjalannya waktu. Perkembangan tersebut terjadi karena individu telah memiliki pengalaman dalam menyelesaikan tugas atau kegiatannya melalui penggunaan internet (Candra Wulan et al., 2022 dalam Ardiansyah, H., & Amalia, R., 2023).

Pada era digital saat ini, remaja sering menggunakan gadget untuk mengakses media sosial, menonton video, bermain game, dan browsing internet. Namun, mereka seringkali tanpa sadar membagikan data pribadi di media sosial, yang berisiko disalahgunakan oleh pihak tidak bertanggung jawab. Kesadaran akan bahaya kebocoran data pribadi sangat penting bagi remaja untuk melindungi privasi dan keamanan mereka. (Fredlina, 2021 dalam Susanti et al., 2022). Selain itu, para remaja juga banyak menggunakan aplikasi perbelanjaan (*e-commerce*) untuk membeli barang-barang secara *online*. Penggunaan *e-commerce* memanglah memberikan kemudahan bagi masyarakat untuk berbelanja tanpa bepergian jauh, tetapi juga menimbulkan resiko keamanan data pribadi. Data pribadi tersebut seperti nama, alamat, nomor telepon, dan informasi keuangan bisa dengan mudah dicuri atau disalahgunakan oleh pihak yang tidak bertanggung jawab. Ancaman keamanan data pribadi pada pengguna *e-commerce* dapat berupa serangan *malware, phishing, hacking,* dan pencurian identitas (Kehista et al., 2023). Dalam penggunaan internet untuk *browsing*, pada platform atau situs tertentu terkadang banyak sekali iklan atau tautan yang tidak jelas. Situs tersebut mendorong penggunanya untuk mengklik tautan sehinggadapat menimbulkan resiko kebocoran data pribadi. Sehingga, diperlukannya upaya penumbuhan rasa kesadaran terhadap peningkatan literasi keamanan digital dan perlindungan data pribadi kepada masyarakat, khususnya para remaja yang rentan dalam penggunaan teknologi.

Permasalahan-permasalahan tersebut mendorong kami untuk melakukan pengabdian kepada masyarakat terkait pentingnya perlindungan data pribadi. Adapun kegiatan pengabdian ini yang kami laksanakan di SMP Negeri 4 Kota Tasikmalaya. Tujuan dari kegiatan kami yaitu untuk bisa memberikan informasi yang bermanfaat terkait pentingnya peningkatan literasi keamanan digital dan perlindungan data pribadi bagi siswa untuk meningkatkan pemahaman peserta didik dalam menggunakan media sosial dan pentingnya menjaga privasi dan keamanan data pribadi.

METODE

Metode pelaksanaan yang digunakan dalam kegiatan pengabdian ini menggunakan tiga tahap, yaitu tahap persiapan, tahap pelaksanaan, dan tahap evaluasi. Kegiatan pengabdian yang dilakukan di SMPN 4 Kota Tasikmalaya mengenai "Pentingnya Peningkatan Literasi Keamanan Digital bagi Siswa SMPN 4 Kota Tasikmalaya untuk Melindungi Data Pribadi", dengan sasaran yaitu peserta didik kelas 8J.

A. Tahap Persiapan

Pada tahap ini menentukan ide dan jenis kegiatan yang akan dilaksanakan yakni berupa kegiatan pengabdian dengan tema "Pentingnya Peningkatan Literasi Keamanan Digital bagi Siswa SMPN 4 Kota Tasikmalaya untuk Melindungi Data Pribadi". Selanjutnya menentukan tempat pelaksanaan kegiatan. Kegiatan ini akan dilaksanakan di SMPN 4 Kota Tasikmalaya. Kemudian menentukan perangkat kegiatan yang diperlukan dalam kegiatan.

B. Tahap Persiapan

Pada tahap pelaksanaan, adanya proses pembuatan proposal kegiatan, yakni menguraikan rancangan terkait kegiatan. Kemudian persiapan pelaksanaan kegiatan, yakni melaksanakan permintaan izin kepada pihak lembaga untuk melaksanakan kegiatan. Setelah adanya perizinan, selanjutnya adalah tahap pelaksanaan kegiatan, yakni melaksanakan sosialisasi mengenai "Pentingnya Peningkatan Literasi Keamanan Digital bagi Siswa SMPN 4 Kota Tasikmalaya untuk Melindungi Data Pribadi". Adapun waktu dan tempat pelaksanaanya sebagai berikut:

Tanggal Pelaksanaan : 06 November 2024
Tempat Pelakasanaan : SMPN 4 Kota Tasikmalaya

C. Tahap Evaluasi

Tahap evaluasi adalah tahap akhir dalam pelaksanaan kegiatan, pada tahap ini dilaksanakannya proses mengukur keberhasilan dari kegiatan. Kami membuat *google form* untuk mengukur seberapa jauh pemahaman peserta didik terhadap materi yang disampaikan mengenai perlindungan data pribadi. Kemudian menyusun laporan akhir hasil kegiatan dari yang sudah didapatkan pada saat tahap pelaksanaan kegiatan berupa karya ilmiah atau artikel yang kemudian di-*submit* ke jurnal yang akan dituju.

HASIL DAN PEMBAHASAN

Lemahnya pelindungan data pribadi di Indonesia mengakibatkan maraknya kebocoran data. Terbukti dengan sering terjadinya kasus kejahatan *cyber*, seperti *hacking* (peretasan) maupun *cracking* (pembajakan) media sosial yang berujung pada pembobolan data pribadi, pemerasan hingga penipuan daring. Mengutip pernyataan Dirjen Aplikasi Informatika, Samuel A. Pangerapan, terdapat lima alasan utama pentingnya menjaga data pribadi, yaitu mencegah intimidasi online terkait gender, mencegah penyalahgunaan data pribadi oleh pihak yang tidak bertanggung jawab, menjauhi potensi penipuan, menghindari potensi pencemaran nama baik, dan hak kendali atas data pribadi. Berdasarkan hasil analisis yang kami lakukan, dapat diketahui bahwa data pribadi dalam Peraturan Menkominfo No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik Data Pribadi adalah data perseorangan tertentu yang disimpan, dirawat dan dijaga kebenaran serta dilindungi kerahasiaannya. Menurut (Haroen, 2014 dalam Lutfi. R, 2022) data pribadi adalah sebuah informasi nyata dan otentik yang terletak pada seseorang sehingga bisa mengidentifikasi orang tersebut. Sedangkan menurut (Rosadi, S. D, 2016) data pribadi penting untuk dilindungi karena untuk memastikan bahwa data pribadi yang dikumpulkan oleh individu digunakan sesuai dengan tujuan pengumpulan nya, sehingga dapat menghindari penyalahgunaan data pribadi. Maka dapat disimpulkan data pribadi adalah data yang berupa identitas dan penanda personal yang bersifat pribadi.

Perlindungan data pribadi saling berkitan dengan privasi, menurut Thmas J. dan Imedinghaff dalam (Benuf et al. 2019) mengemukakan bahwa konsep dari privasi adalah suatu data atau informasi yang dimiliki oleh seseorang dengan dikumpulkan dan dijaga agar tidak digunakan oleh orang lain.

Perlu kita ketahui bahwa upaya perlindungan terhadap data pribadi adalah suatu tindakan yang dilakukan oleh seseroang agar bisa mewujudkan keamanan privasi yang dimilikinya. Menurut (Veritasia, M. E., 2015) dalam perlindungan pribadi aspek privasi dikaji dalam dua bagian, yakni privasi secara psikologis dan privasi secara fisik. Menurut Kurniullah et al. (2021) aspek privasi psikoogis adalah segala aspek privasi yang memiliki katian dengan kondisi pikiran manusia, seperti rencana, keyakinan yang dimiliki, dan suatu yang diinginkan oleh manusia tersebut. Sedangkan aspek privasi fisik adalah aspek privasi yang lebih berkaitan dengan aktivitas manusia secara fisiknya seperti dalam memperlihatkan kehidupan pribadinya.

Dapat disimpulkan bahwa definisi perlindungan data pribadi salah satunya menurut (Westin. A, 1967 dalam Djafar, 2019) adalah data yang merupakan privasi yang terkait dengan data dan informasi pribadi yang dimiliki seseorang yang menjadi hak untuk pertama kalinya, dan menjadi privasi seseorang dalam berkomunikasi maupun tidak berkomunikasi dengan orang lain. Dalam UU RI Pasal 28 G Ayat 1 tentang Hak Asasi Manusia, menyatakan bahwa setiap warga negara berhak atas perlindungan data pribadi, hak-hak pribadi merupakan hal yang bersifat sensitif karena hal tersebut menjadi privasi bagi seseorang dalam data atau informasi yang dimiliki seseorang seperti halnya Kartu Tanda Penduduk (KTP), Paspor, Surat Izin Mengemudi (SIM), Kartu Keluarga (KK), Nomor Pokok Wajib Pajak (NPWP), Nomor Rekening Bank, dan juga sidik jari.

Untuk mengetahui terkait perlindungan data pribadi di lingkungan siswa, kami melakukan kegiatan pengabdian yang kami lakukan dengan judul "Peningkatan Literasi Keamanan Digital dan Perlindungan Data Pribadi bagi Siswa SMPN 4 Kota Tasikmalya" sudah dilaksanakan pada hari Rabu tanggal 06 November 2024 dari pukul 07.30 s.d 09.30 WIB. Kegiatan ini berlangsung dengan baik dan lancar serta mendapatkan respon yang positif dari pihak sekolah dan peserta didik.

Gambar 1.
Foto bersama setelah kegiatan pengabdian

Adapun hasil dari pengabdian yang kami lakukan yaitu siswa kelas 8 j berjumlah 35 orang mereka merespon dan menyambut kami dengan penuh semangat. Suasana kelas yang hangat dan interaktif pun tercipta. Ketika proses penyampaian materi terdapat beberapa siswa yang merespon pertanyaan yang kami ajukan terkait perlindungan data dengan jawaban yang sudah sesuai, hanya saja mereka masih mengetahui dasarnya. Seperti mengetahui data pribadi apa saja, dan penggunaan kata sandi di hp. Namun, beberapa dari mereka belum mengetahui secara lebih dalam terkait pentingnya perlindungan data pribadi di online.

Gambar 2.
Praktik dan pengecekan keamanan HP siswa

Adapun respon siswa terkait seberapa jauh pemahaman tentang perlindungan data pribadi, hal itu kami dapatkan melalui post test yang telah dibuat pada google form, sebagai berikut:

Gambar 3.
Pengetahuan individu terhadap data pribadi

Gambar 4.
Pandangan individu terkait pentingnya perlindungan data pribadi

Gambar 5.
Pengetahuan individu terhadap data pribadi online yang harus dijaga

Pada saat pengabdian, kami juga menanyakan terkait pengalaman mereka apakah mereka pernah mengalami masalah kebocoran data atau tidaknya. mereka memberikan respon, bahwa beberapa dari mereka pernah mengalami masalah-masalah tersebut seperti ada yang menerima paket tanpa dipesan, menerima spam telepon dari nomor yang tidak dikenal, menerima pesan yang mengatasnamakan artis dan stasiun tv, dan orang tuanya ada yang pernah dibobol ATM nya.

Berdasarkan masalah-masalah tersebut, agar tidak terulang kembali, Menurut (Fajri, 2022) ada beberapa cara dalam mencegah kebocoran data, diantaranya:

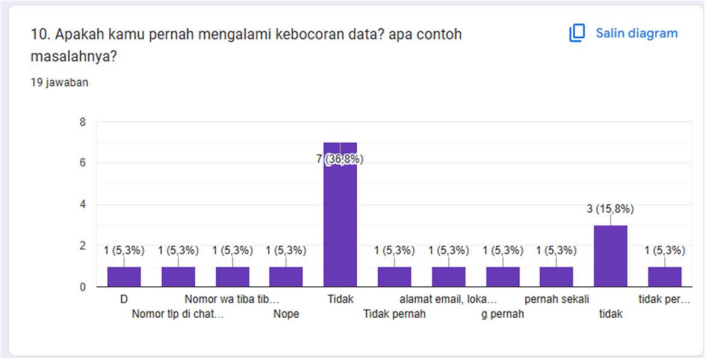
1. Mewaspadai wifi umum

   Langkah pertama dalam pencegahan kebocoran data pribadi adalah dengan menghindari penggunaan wifi umum. Yakni dengan menghindari pembukaan aplikasi *mobile banking*, *online shop*, dan *webmail*.
2. Menggunakan *software* asli

   Langkah kedua adalah menghindari penggunaan software bajakan yang rentan terkena *malware*.
3. Menghindari situs/*link phising*

   Langkah ketiga adalah menghindari website berbahaya.
4. Rutin mengubah *password*

   Langkah ke empat adalah rutin mengubah password dalam berbagai akun pada saat penggunaan gawai, seperti *email*, *mobile banking*, media sosial, pin ATM dengan menggunakan kata sandi yang sulit untuk ditebak.



Gambar 6.
Studi kasus yang dialami oleh peserta didik

Kami juga melakukan *survey* untuk mengetahui setelah adanya informasi yang mereka peroleh dari pengabdian ini apakah membuat mereka semakin hati-hati dan lebih tahu bagaimana cara

menjaga data pribadi. Kemudian, respon mereka menunjukan bahwa setelah adanya kegiatan pengabdian terkait pentingnya perlindungan data pribadi mereka semakin hati-hati.

Gambar 7.
Pandangan individu setelah diadakannya kegaitan pengabdian

Salah satu upaya yang harus dilakukan dalam melindungi data pribadi yaitu dengan menjaga keamanan kata sandi pribadi. Adapun beberapa cara untuk membuat kata sandi atau password yang kuat agar aman dari kebocoran data, menurut (Dewaweb team, 2023) sebagai berikut :

1. Menggunakan kata sandi berbeda-beda di setiap akun
   Menggunakan kata sandi yang berbeda-beda di setiap akun memungkinkan pengguna untuk menghindari terjadinya pembajakan secara sekaligus di setiap akun ketika kata sandi yang dimiliki oleh seseorang diketahui oleh orang lain.
2. Menghindari bentuk kata sandi yang mudah ditebak
   Menggunakan bentuk kata sandi yang mudah ditebak adalah salah satu kesalahan yang sering dilakukan oleh banyak orang seperti *"qwerty"*, *"12345678"*, atau *"admin#123"*, karena orang lain bisa saja mengetahui kata sandi yang digunakan oleh seseorang dari informasi yang diunggah oleh orang tersebut di media-media online.
3. Rahasiakan dan amankan kata sandi
   Merahasiakan kata sandi ataupun *username* kepada siapapun meskipun orang terdekat sekalipun, ataupun tidak membeberkan *username* dan kata sandi di tempat umum.
4. Menggunakan kata sandi generator dan manajer
   Kata sandi generator dan manajer adalah *tools* yang berfungsi untuk menghasilkan kata sandi secara otomatis, kata sandi yang kuat biasanya terdiri dari huruf besar dan kecil, angka, hingga karakter khusus, alat ini biasanya sudah tersedia di pengguna akun *google*.
5. Mematuhi syarat kata sandi yang kuat
   Sebuah aplikasi biasanya merekomendasikan beberapa syarat pembuatan kata sandi yang harus dipatuhi agar keamanan akun terjamin, seperti menggunakan huruf besar, huruf kecil, angka, simbol atau tanda baca khusus.
6. Mengaktifkan verifikasi 2 langkah
   Verifikasi 2 langkah berfungsi sebagai langkah kedua setelah memasukan kata sandi, alat ini sudah banyak diterapkan pada layanan *online* seperti media sosial, *email*, *mobile banking*, dan sebagainya.
7. Memperbaharui *software*
   Sebagian besar aktivitas *hacker* menargetkan celah atau kerentanan yang terdapat pada *softwar*e. Sehingga pengguna gawai harus sering memperbaharui *software* ke versi terbaru, guna memperbaiki *bug* dan kerentanan yang ada sebelumnya dalam *software*.
8. Menggunakan kata sandi pada semua gawai

Setiap gawai yang dimiliki oleh seseorang diusahakan menggunakan kata sandi untuk mencegah akses tanpa izin dari pihak ketiga.

9. Mengubah kata sandi secara rutin

   Mengubah kata sandi dapat mencegah akses pihak ketiga yang mengetahui kata sandi sebelumnya, selain itu mengganti kata sandi juga bermanfaat untuk memastikan akun tetap aman dan sulit untuk diretas.

Selain menjaga keamanan kata sandi, menjaga keamanan email merupakan upaya penting yang harus diperhatikan dalam perlindungan data pribadi . Menurut Eicon Technology,2019 terdapat enam cara untuk menjaga keamanan email, yaitu:

1. Mengaktifkan fitur verifikasi dua Langkah

   Yaitu suatu fitur yang digunakan dengan cara meminta provider atau email mengirimkan kode ke ponsel agar terhindar dari orang asing yang ingin mengakses email, karena dengan fitur ini belum tentu bisa login lantaran harus mengisi kode yang dikirimkan ke ponsel pengguna email.
2. Mengubah browser kepada versi yang lebih modern

   Upaya selanjutnya adalah dengan cara menggunakan browser versi terbaru akan memperbaiki kekurangan sebelum merubah browser ke versi terbaru, sehingga dapat membantu mengamankan email.
3. Menghindari membuka email tak dikenal

   Dengan cara meminta untuk membuka email tak dikenal pengirimnya dan klik sesuatu pada email yang dikirimkan ke ponsel, merupakan salah satu cara seseorang yang berniat hack email pribadi diponsel kita.
4. Menghindari pengisian form web mencurigakan

   Dengan memberikan penawaran menarik seperti berupa menonton film secara gratis, atau video-video secara gratis, dengan mengarahkan untuk mengisi form tersebut dan harus mencantumkan email serta kata sandi, maka berhati-hatilah agar email yang kita kirimkan tidak disalahgunakan.
5. Memilih provider yang teruji keamanannya

   Ketika akan memilih provider pastikan memilih provider yg telah teruji keamananya dan sangat menjaga data penggunanya misalnya layanan milik Google yaitu Gmail.
6. Menggunakan kata sandi dengan alfanumerik

   Gunakan kata sandi dengan menggunakan huruf kapital di awal kemudian menambahkan angka, tanda hubung, dan kode-kode unik dan pastikan sering mengubah kata sandi agar terhindar dari hal-hal yang tidak diinginkan.

KESIMPULAN

Perlindungan data pribadi merupakan hal yang sangat penting untuk bisa diketahui oleh Masyarakat di era modern saat ini. Di tengah media sosial yang digunakan oleh semua kalangan, terkhusus pada anak remaja saat ini perlu adanya peningkatan literasi keamanan digital dan perlindungan data pribadi. Hal tersebut dibuktikan dari adanya kegiatan pengabdian yang kami lakukan di SMPN 4 Kota Tasikmalaya, yang menghasilkan respon dari peserta didik terkait cara mereka menjaga keamanan data pribadi mereka dalam penggunaan gadget. Rata-rata peserta didik dari mereka sudah paham akan pentingnya menjaga keamanan data pribadi. Namun, ada juga dari beberapa peserta didik pernah mengalami kebocoran data pribadi sebagai akibat dari kurang pahamnya peserta didik dalam menjaga data pribadi. Dari permasalahan tersebut pastinya ada pencegahan yang dapat dilakukan oleh individu khususnya peserta didik agar data pribadi yang dimiliki tidak bocor, seperti menghindari pembukaan aplikasi penting menggunakan wifi umum, menggunakan *software* bawaan dari gadget, menghindari situs atau link yang tidak jelas tujuannya, dan rutin mengubah password akun-akun penting yang digunakan dalam gadget. Kami berharap dengan adanya pengabdian ini peserta didik dapat lebih peduli terhadap perlindungan data pribadi

secara elektrobik maupun elektronik. Saran dari kami, semoga pihak sekolah kedepanya bisa sering mengadakan kegiatan edukasi terkait perlindungan data pribadi kepada seluruh siswa, agar mereka lebih bisa memahami secara mendalam.

UCAPAN TERIMA KASIH

Kami bersyukur atas kehadirat Tuhan Yang Maha Esa atas berkatNya dierikan kelancaran serta kemudahan kepada penulis untuk dapat menyelesaikan jurnal dengan judul "Peningkatan Literasi Keamanan Digital dan Perlindungan Data Pribadi bagi Siswa SMPN 4 Kota Tasikmalaya". Penulis juga mengucapkan terimakasih kepada semua rekan yang terlibat dalam pembuatan jurnal ini. Tak lupa penulis juga mengucapkan terimakasih kepada peneliti terdahulu sehingga karyanya dapat digunakan referensi dalam pembuatan jurnal ini. Selain itu kami mengucapkan terimakasih kepada Bpk. Ahmad Hamdan selaku dosen pembimbing yang selalu memberikkan motivasi dan dukungan kepada penulis dan juga penulis berterimakasih kepada pihak SMPN 4 Kota Tasikmalaya yang sudah memfasilitasi kami dalam kegiatan pengabdian.

DAFTAR PUSTAKA

Ardiansyah, H., & Amalia, R. (2023). Pengenalan Cyber Security Untuk Pesertadidik SMP Muhammadiyah Parakan Di Era Society 5.0. Jurnal Indimas, 1(1), 9-3.

Benuf, K., Mahmudah, S., & Priyono, E. A. (2019). Perlindungan Hukum Terhadap Keamanan Data Konsumen Financial Technology di Indonesia: Indonesia. Refleksi Hukum: Jurnal Ilmu Hukum, 3(2), 145–160.

Dewaweb team. (2023). 10 Cara Membuat Password yang Kuat Agar Aman dari Hacker. Dewaweb. Diakses dari: https://www.dewaweb.com/blog/cara-membuat-password-yang-kuat/

Djafar, W. (2019). Hukum perlindungan data pribadi di indonesia: lanskap, urgensi dan kebutuhan pembaruan. In Seminar Hukum dalam Era Analisis Big Data, Program Pasca Sarjana Fakultas Hukum UGM (Vol. 26). 1-14.

EIKON Technology. (2019). 6 Langkah Meningkatkan Keamanan Email Dari Serangan Cyber. EIKON Technology. Diakses dari: https://blog.eikontechnology.com/keamanan-email/.

Fajri, D. L. (2022). 4 cara mencegah kebocoran data pribadi. Katadata. Diakses dari: https://katadata.co.id/berita/nasional/6316e77ce470b/4-cara-mencegah-kebocoran-data-pribadi.

Febriansyah, F., & Muksin, N. N. (2020). Fenomena Media Sosial: Antara Hoax, Destruksi Demokrasi, dan Ancaman Disintegrasi Bangsa. Sebatik, 24(2), 93-200.

Haroen, D. (2014). Personal branding. Gramedia Pustaka Utama.

Imedinghaff, Thomas J., ed., Online Law The SPA's Legal Guide to Going Business on The Internet (Addison-wesley Developers Press 1996).

Kehista, A. P., Fauzi, A., Tamara, A., Putri, I., Fauziah, N. A., Klarissa, S., & Damayanti, V. B. (2023). Analisis Keamanan Data Pribadi pada Pengguna E-Commerce: Ancaman, Risiko, Strategi Kemanan (Literature Review). Jurnal Ilmu Manajemen Terapan, 4(5), 625-632.

Kurniawan, I., Hartadi, G., Olivia, F., Judge, Z., Siswanto, A. H., Suprayogi, A., & Slamet, R. (2022). Penyuluhan Aspek Hukum Perlindungan Privasi dan DataPribadi. Jurnal Abdimas, 8(5), 308-34.

Kurniullah, A. Z., Simarmata, H. M. P., Sari, A. P., Sisca, S., Mardia, M., Lie, D., Anggusti, M., Purba, B., Mastuti, R., & Dewi, I. K. (2021). Kewirausahaan dan Bisnis. Yayasan Kita Menulis.

Luthfi, R. (2022). Perlindungan Data Pribadi sebagai Perwujudan Perlindungan Hak Asasi Manusia. Jurnal Sosial Teknologi, 2(5), 431-436.

Menkominfo. (2016). Peraturan tentang Perlindungan Data Pribadi dalam Sistem Elektronik Data Pribadi.

Rosadi, S. D. (2016). Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia. Yustisia, 5(1), 35-53.

Susanti, M. D. E., Palupi, G. S., Nerisafitra, P., & Wibawa, R. P. (2022). Sosialisasi Dan Pelatihan Tentang

Privacy Dan Keamanan Internet Pada Peserta Didik Smp Negeri 1 Waru. Prosiding Seminar Nasional Pengabdian Kepada Masyarakat, 2(1), 489–498.

Veritasia, M. E. (2015). Pengungkapan Informasi Privat tentang Identitas Seksual Seorang Gay kepada Orang Lain. Universitas Airlangga. 1-39.

Westin, A. (1967). Privacy and freedom new york atheneum, 1967. Privacy and Personnel Records, The Civil Liberties Review (Jan./Feb., 1976) S, 28–34.