

## **BAB 6**

---

# **KEAMANAN INFORMASI DAN ETIKA DIGITAL**

*Eri Riana*

### **A. Pendahuluan**

Era internet disaat ini, informasi mudah diperoleh dan disebarluas (Maryanto et al., 2022). Oleh sebab itu, informasi menjadikan aset yang berharga baik bagi individu, swasta ataupun pemerintah (Nasution, 2018). Informasi mempunyai nilai yang harus dilindungi (Saputra et al., 2023), sehingga penting bagi individu dalam melakukan perlindungan terhadap informasi.

### **B. Konsep Dasar Keamanan Informasi**

Keamanan informasi (Islami et al., 2024) merupakan suatu cara yang merujuk pada perlindungan informasi dari penggunaan, akses, gangguan, perubahan, inspeksi, modifikasi, pencatatan atau perusakan yang tidak sah. Tujuan menerapkan keamanan informasi adalah untuk menjaga kerahasiaan, integritas dan ketersediaan informasi ataupun data yang mencakup suatu langkah-langkah yang dirancang dalam pencegahan pelanggaran keamanan di mana informasi disimpan secara fisik dan elektronik. Menjaga supaya

informasi sensitif tetap tersembunyi dari orang yang tidak berhak untuk mengakses, memastikan hanya individu yang berhak yang bisa mengakses informasi. Serta memastikan bahwa informasi lengkap dan akurat, dan bahwa tidak ada suatu modifikasi tidak sah terhadap data, baik secara sengaja ataupun tidak sengaja. Menjamin informasi serta sumber daya terkait bisa diakses oleh setiap individu yang berhak disaat dibutuhkan. Penerapan keamanan informasi melibatkan teknologi keamanan fisik, elektronik, prosedur, dan *policy* manajemen komprehensif yang didalamnya terdapat adanya penggunaan enkripsi, *firewall*, *antivirus*, autentikasi dan manajemen akses. Keamanan informasi menjadi penting seiring dengan peningkatan ancaman (Habibah, 2024) di dunia *cyber* seperti *phising*, *malware*, dan serangan *ransomware*, dan adanya kebutuhan untuk mematuhi peraturan dalam perlindungan data yaitu *General Data Protection Regulation* (GDPR) di Uni Eropa serta berbagai Undang-Undang perlindungan data di seluruh dunia. Keamanan informasi adalah aspek kritis di mana informasi dan data menjadikan aset yang berharga bagi individu, bisnis dan pemerintah.

### **C. Prinsip Dasar Keamanan Informasi**

Berikut ini adalah beberapa prinsip (Nurul et al., 2022) mendasar keamanan informasi (Bengkalis, 2024):

#### **1. Kerahasiaan (*Confidentiality*)**

Kerahasiaan (*confidentiality*) di dalam keamanan informasi terkait pada perlindungan informasi supaya dapat diakses dengan pihak berwenang, dengan memastikan data sensitif dapat terlindungi dari akses yang tidak berhak atau mengungkapkan kepada pihak yang tidak berhak. Implementasi kerahasiaan (*Confidentiality*) dengan menerapkan strategi dan teknologi seperti

enkripsi, kontrol akses, pelatihan kesadaran keamanan, penggunaan *Virtual Private Networks* (VPN), dan perjanjian hukum seperti *Non-Disclosure Agreements* (NDA).

## 2. Integritas (*Integrity*)

Integritas di dalam konteks keamanan informasi merujuk kepada perlindungan informasi dari modifikasi yang tidak sah, baik secara disengaja ataupun tidak disengaja. Dalam hal ini untuk menjamin bahwa suatu data tetap lengkap dan akurat sepanjang daur siklus hidupnya. Integritas memastikan data tidak berpengaruh dalam suatu perubahan yang tidak sah sehingga dapat hilang integritasnya. Untuk memastikan penerapan integritas data, perusahaan atau organisasi mengimplementasikan berbagai teknik dan kontrol seperti kontrol akses, penggunaan dalam fungsi *hash*, tanda tangan digital, manajemen *patch*/pembaharuan dan audit/*logging*. Kenapa integritas sangat penting?, integritas sangat penting di mana bisa menumbuhkan atau membangun rasa kepercayaan dari pengguna, pelanggan atau mitra bisnis. Integritas juga sebagai pemenuhan terhadap suatu regulasi serta untuk pengambilan keputusan bisnis yang akurat dan tepat waktu di mana semuanya bergantung kepada data yang akurat serta lengkap. Kerusakan dalam integritas data bisa menimbulkan kerugian reputasi dan finansial.

## 3. Ketersediaan (*Availability*)

Ketersediaan dalam konteks keamanan informasi menjamin informasi, sistem dan *resource* selalu bisa diakses saat diperlukan dan digunakan oleh pihak yang berhak mengakses kapan pun dibutuhkan. Prinsip ketersediaan menekankan kepada pentingnya memastikan data, informasi, aplikasi, dan sumber daya informasi teknologi lainnya selalu tersedia untuk

operasional bisnis yang berkelanjutan (*business continuity*), tanpa gangguan apapun. Untuk memastikan penerapan ketersediaan, Perusahaan atau organisasi harus menerapkan berbagai teknik dan strategi seperti Redundansi dan *Failover*, *Backup Data*, Pemulihan Bencana (*Disaster Recovery*), Pengukuran Kinerja dan Monitoring, dan Pemeliharaan dan Pembaruan. Kenapa ketersediaan sangat penting?, ketersediaan sangat penting untuk kontinuitas bisnis, kepatuhan regulasi, dan kepuasan dari pengguna.

#### **D. Perlindungan Data Pribadi (PDP)**

Perlindungan data pribadi (Mita Baqis et al., 2025) merupakan serangkaian upaya untuk melindungi data dan informasi yang terlekat pada diri seseorang (seperti nama lengkapnya, NIK, alamat, hingga pendidikan, riwayat kesehatan dan lain-lain) dari suatu penyalahgunaan dan suatu akses tidak sah. Tujuannya untuk menjamin hak privasi dan memberikan kontrol penuh kepada pemilik data atas informasi yang dimiliki.

Dengan terdapatnya peningkatan pengumpulan data individu oleh organisasi, keamanan informasi bisa membantu dalam perlindungan privasi data individu dan pencegahan terjadinya pengambilan identitas pribadi. Peraturan semacam (GDPR) dan Undang-Undang perlindungan data di seluruh dunia ditekankan perlunya keamanan informasi dalam kepatuhan hukum. Di Indonesia, perlindungan data pribadi diatur secara spesifik melalui

|                                                        |
|--------------------------------------------------------|
| Undang-Undang Pelindungan Data Pribadi (UU PDP) No. 27 |
|--------------------------------------------------------|

|            |
|------------|
| Tahun 2022 |
|------------|

 Undang-Undang ini membagi konsep perlindungan ke dalam beberapa aspek sebagai berikut:

### 1. Jenis Data Pribadi

Berdasarkan hukum yang berlaku, data pribadi dibagi dua kategori:

- a. Data yang bersifat umum: Nama lengkap, jenis kelamin, kewarganegaraan, agama, dan data pribadi yang dikombinasikan untuk mengidentifikasi seseorang.
- b. Data yang bersifat spesifik: Data dan informasi kesehatan, data biometrik, genetika, catatan kejahatan, data anak, data keuangan pribadi, dan data spesifik lainnya.

### 2. Hak Pemilik Data

Sebagai subjek atau pemilik data pribadi, pemilik data memiliki hak penuh untuk:

- a. Memperoleh informasi tentang tujuan penggunaan data pemilik.
- b. Memperbaharui atau memperbaiki kesalahan pada data pemilik.
- c. Meminta penghapusan atau pemusnahan data jika tidak lagi diperlukan.
- d. Menarik kembali semua persetujuan pemrosesan data kapan saja.
- e. Mengajukan gugatan dan meminta ganti rugi jika terjadi penyalahgunaan data.

### 3. Kewajiban Pengelola Data

Perusahaan, institusi pemerintah, dan organisasi yang bertindak sebagai pengendali dan pemroses data memiliki suatu kewajiban hukum untuk:

- a. Mendapatkan persetujuan secara sah dari pemilik data sebelum mengumpulkan dan mempergunakannya.
  - b. Menyediakan sistem keamanan yang kuat untuk mencegah terjadinya kebocoran data.
  - c. Menjaga kerahasiaan dan memproses data agar sesuai dengan tujuan awal yang sudah disepakati.
4. Sanksi Hukum Pelanggaran

Penyalahgunaan data pribadi, seperti menjual data tanpa seizin pemilik data, kebocoran data akibat kelalaian sistem/kelalaian manusia, atau pemalsuan terhadap data, dapat dikenakan sanksi hukum. Berdasarkan UU PDP, pelanggar bisa dikenakan denda yang sangat besar hingga sanksi pidana penjara.

## **E. Etika Digital**

Etika digital adalah kumpulan dari norma (Papua et al., 2025), nilai-nilai, aturan-aturan, norma moral yang mengatur perilaku individu dalam mempergunakan teknologi digital supaya tidak merugikan orang lain atau merugikan diri pribadi. Etika digital sangat berkaitan mengenai tanggung jawab (Putri et al., 2026), kesadaran, serta perilaku etis dalam berinteraksi menggunakan teknologi, seperti mempergunakan internet, mempergunakan media sosial, mempergunakan perangkat elektronik, dan mempergunakan aplikasi digital. Sehingga prinsip dari suatu etika digital yaitu menghormati orang lain, menghargai akan karya cipta intelektual, jujur, dan bertanggung jawab. Etika digital menjadi hal yang sangat perlu sebab berkaitan dengan teknologi yang sudah menjadi bagian dalam kehidupan sehari-hari. Di bawah ini merupakan perlunya kita tahu mengenai etika digital:

1. Perlindungan Privasi

Etika digital sangat mencermati, memikirkan hak dari privasi setiap individu serta perlindungan terhadap data pribadi (PDP). Dengan adanya etika digital, bisa terhindar dari pelanggaran privasi, contohnya pengambilan dari identitas pribadi orang serta pelanggaran penggunaan informasi data individu (Merdiaty et al., 2025).

2. Perlindungan dan Keamanan

Etika digital berfungsi untuk keamanan dalam dunia digital. Hal tersebut termasuk dalam pencegahan *phishing*, virus, peretasan, *malware*, sistem/web, dan serangan *cyber* sehingga dapat merugikan individu atau perusahaan.

3. Mencegah Penyebaran *Hoax*

Kita mengharapkan dalam pemeriksaan kebenaran akan suatu data informasi sebelum kita menyebarkannya, serta mencegah terjadinya sebaran informasi (*Hoax*) (Prasetyo et al., 2024).

4. Menghindari *Cyberbullying* dan Pelecehan Online

Tidak ikut serta melakukan dalam tindakan perundungan yang dilakukan melalui media digital atau internet. Contohnya:

- a. Merendahkan orang lain, mengejek, menghina di media sosial.
- b. Melakukan pengancaman, melakukan intimidasi di media online.
- c. Menyebarkan video, foto ataupun informasi pribadi orang lain tanpa sepengetahuan pemilik informasinya.

d. Mengkerdikan/mengucilkan orang lain dalam suatu grup chat di *whatsapp* misalnya atau dalam suatu komunitas digital.

#### 5. Dampak Secara Moral dan Sosial

Hal ini terkait dengan pertimbangan bagaimana suatu perilaku *online* bisa berpengaruh kepada masyarakat, orang lain, serta lingkungan sekitarnya.

#### 6. Membentuk Digital Identitas.

Etika digital akan membentuk suatu identitas digital profesional serta positif. Melalui kepatuhan dalam etika digital, bisa menumbuhkan suatu reputasi *online* dan bisa menciptakan suatu hubungan yang sehat.

#### 7. Bertanggung jawab dalam mempergunakan teknologi informasi.

Dengan etika digital menciptakan dalam penggunaan teknologi secara bijaksana dan bertanggung jawab. Hal tersebut tercakup dalam penggunaan secara berimbang, menghindari terjadinya berlebihan, serta ketergantungan dengan menyadari terhadap dampak terhadap fisik dan mental.

Dengan etika digital dapat membuat lingkungan *online* yang beretika, aman, serta bermanfaat untuk yang menggunakannya. Melalui pemahaman serta penerapan etika digital, kita dapat memanfaatkan teknologi dengan lebih baik dan tidak menimbulkan resiko atau dampak yang negatif.

Di bawah ini merupakan contoh prinsip-prinsip di dalam pengolahan konten digital supaya sesuai dengan prinsip etika digital dan tidak akan menjadi konten digital bersifat negatif.

- a. Mempertimbangkan Terlebih Dahulu Sebelum Melakukan Tindakan Posting.

Mempertimbangkan dampak dari konten yang dibuat atau yang akan dibagikan sebelum melakukan posting. Tanyakan kepada diri pribadi apakah konten itu mempromosi suatu toleransi, atau suatu dialog yang sehat, atautkah justru bisa memprovokasi suatu perselisihan dan konflik. Kita harus memperhatikan mengenai kode Etik Jurnalistik di dalam membuat suatu postingan di media sosial.

- b. Fakta dan Kebenaran

Memastikan konten yang di bagikan berdasarkan pada fakta yang bisa diverifikasi akan kebenarannya. Dilarang untuk menyebarkan informasi palsu, atau hoaks, atau suatu klaim yang tidak mempunyai dasar kuat. Verifikasikan terlebih dahulu informasi sebelum membagikannya serta mempergunakan sumber yang terpercaya. Hal ini dapat dihindari dengan cara:

- 1) Cek berita dari sumber resmi dan media yang terpercaya.
- 2) Edukasi orang agar bijak untuk menerima suatu informasi.
- 3) Mencegah pesan berantai yang belum tentu jelas kebenarannya.

- c. Menghargai Privasi

Menjaga *privacy* orang lain di dalam konten digital yang dibuat dan yang disebar. Menghindari pengungkapan informasi pribadi tanpa izin dan menghindari pencemaran terhadap *privacy* orang lain dengan membagikan informasi

sehingga bisa mencemarkan orang lain. *Privacy* orang lain yang dimaksudkan, yaitu data individu.

d. Keadilan dan Keberimbangan.

Memastikan konten yang dibuat atau yang dibagikan objektif, adil, dan seimbang. Menghindari penyampaian informasi yang merugikan atau memihak kepada salah satu pihak secara berlebihan.

Jerat terhadap sangsi hukum terkait dengan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

- a. Pasal 26 (1) dikecualikan dengan ketentuan lain dengan peraturan perundangundangan, dimana setiap penggunaan informasi lewat media elektronik yang tersangkut dengan data pribadi harus melalui persetujuan orang yang terkait. (2) Setiap orang yang melanggar akan haknya sebagaimana dimaksudkan dalam ayat (1) bisa mengajukan gugatan kerugian tersebut.
- b. Tersangka yang menyebarkan data *privacy* bisa dihukum melalui Pasal 32 serta Pasal 48 UU ITE. Ancaman pidana untuk tersangka selama delapan sampai dengan sepuluh tahun dan denda dari Rp 2 miliar sampai dengan Rp 5 miliar.
- c. Perlindungan terhadap data *privacy* ada di dalam Undang-Undang Nomor 27 Tahun 2022 mengenai Pelindungan Data Pribadi (PDP). Peraturan ini adalah produk hukum yang berkaitan dengan PDP yang disahkan tanggal 17 Oktober 2022.

- d. Merujuk pada Pasal 67, di mana setiap orang dengan sengaja melawan hukum dalam mengungkapkan data pribadi yang bukan kepunyaannya dipidana empat tahun penjara atau denda sebesar Rp 4 miliar. Di mana setiap orang sengaja melawan hukum mempergunakan data pribadi yang bukan kepunyaannya akan dipidana selama lima tahun penjara atau denda sebesar Rp 5 miliar.

#### **Pencegahan Terhadap Ujaran Kebencian dan Diskriminasi**

Mencegah konten digital yang bersifat ujaran kebencian, diskriminasi dan pelecehan suatu individu atau golongan berdasarkan agama, gender, orientasi seksual, atau ras. Menjaga sikap inklusif dan bahasa serta menghindari pernyataan sifatnya bisa memprovokasi atau bisa merugikan. Sangat perlu dicatat stigmatisasi, penghinaan, ujaran kebencian, pelecehan, atau pada golongan tertentu dapat menciptakan kerentanan dari sisi yang melakukan posting ataupun dimaksudkan di dalam postingan.

Stigmatisasi merupakan suatu tindakan yang mengeksklusifkan orang atau suatu golongan dibentuk secara sosial. Stigma bisa berupa labelling stereotip, atau diskriminasi yang dapat mempengaruhi diri individu secara keseluruhan. Stigma akan muncul disebabkan masyarakat melihat ada perbedaan dalam diri orang lain ataupun terkait hal yang masyarakat melihat tidak sesuai dengan nilai yang dianut yang harusnya ada di dalam suatu masyarakat.

Ujaran kebencian merupakan suatu tindakan komunikasi dilakukan oleh suatu individu atau suatu kelompok dalam hal memprovokasi, menghasut, atau melakukan penghinaan kepada kelompok atau individu lain dalam berbagai aspek, seperti: ras,

warna kulit, gender, cacat, orientasi seksual, kewarganegaraan, dan agama.

Pelanggaran terhadap konten atau unggahan yang mengandung kebencian dan penghinaan.

Jerat hukum terhadap pelanggaran:

- a. Pada Pasal 243 ayat (1) jo ayat (2) Undang-Undang KUHP yang baru: “Setiap orang yang menyiarkan, mempertunjukkan, atau menempelkan tulisan atau gambar sehingga terlihat oleh umum atau memperdengarkan rekaman sehingga terdengar oleh umum atau menyebarluaskan dengan sarana teknologi informasi, yang berisi pernyataan perasaan permusuhan dengan maksud agar isinya diketahui atau lebih diketahui oleh umum, terhadap satu atau beberapa golongan atau kelompok penduduk Indonesia berdasarkan ras, kebangsaan, etnis, warna kulit, agama, kepercayaan, jenis kelamin, disabilitas mental, atau disabilitas fisik yang berakibat timbulnya kekerasan terhadap orang atau barang, dipidana penjara 4 (empat) tahun atau pidana denda paling banyak kategori IV”.
- b. Pada Pasal 243 ayat (1) jo ayat (2) UU KUHP yang baru: “Jika setiap orang sebagaimana dimaksud pada ayat (1) melakukan tindak pidana tersebut dalam menjalankan profesinya dan pada waktu itu belum lewat 2 (dua) tahun sejak adanya putusan pemidanaan yang telah memperoleh kekuatan hukum tetap karena melakukan tindak pidana yang sama, pelaku dapat dijatuhi pidana tambahan berupa pencabutan hak sebagaimana dimaksud dalam Pasal 86 huruf P’. Memastikan konten digital yang di buat tidak

melanggar hak cipta milik orang. Pasal yang melindungi terkait hak cipta, yaitu Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

- c. Pada Pasal 25 Informasi Elektronik atau Dokumen Elektronik yang tersusun menjadi situs internet, dan karya intelektual yang terdapat di dalamnya dilindungi dalam Hak Kekayaan Intelektual (HKI) berdasar kepada ketentuan didalam Peraturan Perundangan.
- d. Jerat hukumnya, UU Nomor 8 Tahun 2014 mengenai Hak Cipta, tersangka yang melanggar hak cipta akan ditindak tegas dengan denda dan penjara.

Memastikan konten digital yang dibuat atau yang dibagikan sesuai hukum dan peraturan yang sah di ruang digital. Menghindari penyalahgunaan terhadap hak akan kekayaan intelektual, penghinaan, dan perilaku-perilaku ilegal yang lain. Konten digital yang terdapat adanya penyalahgunaan perilaku, misalnya konten digital penyiksaan terhadap hewan, pelanggaran terhadap kesusilaan serta perjudian.

Dengan mengikuti prinsip-prinsip yang sudah dijelaskan diatas kita bisa mengelola konten digital mempergunakan etika yang bagus serta mencegah menghasilkan konten digital yang bersifat negatif.

## **Daftar Pustaka**

- Bengkalis, P. N. (2024). Seminar Nasional Industri dan Teknologi (SNIT), Politeknik Negeri Bengkalis. November, 90–96.
- Habibah, A. N. (2024). Keamanan informasi dalam konteks teknologi komunikasi modern. *Maliki Interdisciplinary Journal (MIJ)* EISSN, 2(6), 965–971. <http://urj.uin-malang.ac.id/index.php/mij/index>
- Islami, L., Akbar, H. P., & Rizal, R. G. (2024). Sistem Keamanan Informasi Di Era Digital. 1(11), 1174–1177.
- Maryanto, A. L., Azam, M. N. A. A., & Nugroho, A. (2022). Evaluation Of Information Security Management In Technology-Based Beginning Company Using The KAMI Index. *Jurnal Simantec*, 11(1), 1–12.
- Merdiaty, N., Saputra, F., Putri, K. A., Syahra, M. N., Setiawan, T. A., & Grace, Y. (2025). Krepa: Kreativitas Pada Abdimas. *Krepa: Kreativitas Pada Abdimas*, 1(3), 35–45.
- Mita Baqis, A., Irwan, M., & Nasution, P. (2025). Pentingnya Perlindungan dan Keamanan Data Privasi di Era Digital. *Jurnal Manajemen Dan Pendidikan Agama Islam*, 3(3), 2025. <https://journal.aripafi.or.id/index.php/jmpai>
- Nasution, M. K. M. (2018). Keamanan Informasi: Pendahuluan. 8(1), 1–2. [https://www.researchgate.net/publication/327542441\\_Keamanan\\_Informasi\\_Pendahuluan](https://www.researchgate.net/publication/327542441_Keamanan_Informasi_Pendahuluan)
- Nurul, S., Shynta Anggrainy, & Siska Aprelyani. (2022). Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review Sim).

- Jurnal Ekonomi Manajemen Sistem Informasi, 3(5), 564–573. <https://doi.org/10.31933/jemsi.v3i5.992>
- Papua, A. P., Safitri, R. A., Amaliah, F., Awwalyah, H., Rahma, A., Alam, N., Informasi, S., Lamappapoleonro, U., Informatika, T., Lamappapoleonro, U., Sipil, T., Lamappapoleonro, U., Lamappapoleonro, U., Lamappapoleonro, U., Sosial, M., Digital, L., & Putro, H. (2025). Pengenalan Etika Digital Untuk Mengurangi Dampak. 3.
- Prasetyo, D. A., Setiawan, F. D., Kapoyos, J. M., Reyhan, M., Hamzah, W., & Fadholi, N. (2024). Pentingnya Etika Siber pada Era Digital. *Nusantara Journal of Multidisciplinary Science*, 2(5), 1130–1137.
- Putri, A. E., Suhandi, N., Informatika, T., Indo, U., Mandiri, G., Informatika, T., Indo, U., & Mandiri, G. (2026). PERAN EDUKASI ETIKA DIGITAL DALAM. 02, 19–25.
- Saputra, A. D., Dione, F., & Uluputty, I. (2023). Pengelolaan Keamanan Informasi dan Persandian di Dinas Komunikasi dan Informatika Provinsi Kalimantan Timur. *Jurnal Teknologi Dan Komunikasi Pemerintahan*, 5(2), 159–187. <https://doi.org/10.33701/jtkp.v5i2.3735>

## **Tentang Penulis**



**Eri Riana, S.T., M.Kom.,** lahir di Cirebon, 21 Mei 1984. Menempuh pendidikan Sarjana (S1) pada Program Studi Teknik Informatika di Universitas Muhammadiyah Cirebon dan lulus pada tahun 2007. Pendidikan Magister (S2) diselesaikan pada bidang Ilmu Komputer di STMIK Nusa Mandiri Jakarta pada tahun 2014. Saat ini penulis sebagai Dosen Tetap di Fakultas Teknik dan Informatika Universitas Bina Sarana Informatika (UBSI) Jakarta, penulis juga aktif sebagai Dosen Tutor di Fakultas Sains & Teknik (FST) di perguruan tinggi negeri Universitas Terbuka (UT) Jakarta.

Penulis memiliki kepakaran dibidang Data Science, Web Technology, Kecerdasan Buatan (AI), Audit IT, Tata Kelola IT dan Keamanan Jaringan. Untuk mewujudkan karir sebagai dosen profesional, penulis pun aktif sebagai peneliti dibidang kepakarannya tersebut. Selain peneliti, penulis juga aktif menulis buku dengan harapan dapat memberikan kontribusi positif bagi bangsa dan negara. Penulis juga aktif selalu memberikan penyuluhan/pelatihan-pelatihan melalui kegiatan pengabdian kepada masyarakat dibidang pendidikan komputer. Penulis bisa dihubungi melalui:

Email Penulis

[eri.eea@bsi.ac.id](mailto:eri.eea@bsi.ac.id)

[04002306@ecampus.ut.ac.id](mailto:04002306@ecampus.ut.ac.id)

Nomor HP/WA

: 0895332850621