BAB V
SIMPULAN, IMPLIKASI, DAN REKOMENDASI

5.1. Simpulan

5.1.1. Simpulan Umum

Di era sekarang ini kemajuan zaman diharapkan dapat berkontribusi positif bagi kemajuan peradaban manusia. Namun, di sela-sela megahnya perkembangan zaman teknologi ini terdapat beberapa penyimpangan yang juga ikut berkambang yaitu kejahatan digital. Dari berbagai tindakan kejahatan di dunia siber salah satunya yaitu *doxing*. *Doxing* ini sendiri merupakan sebuah pelanggaran, penyimpangan, atau kejahatan karena mengungkapkan data pribadi seseorang ke publik tanpa seizin dari pemiliknya. Penyebaran tanpa izin ini bisa menimbulkan kerugian karena sifatnya data pribadi yang privat. *Doxing* ini sendiri dibagi menjadi beberapa kategori yaitu *deanonymizing doxing, targeting doxing, dan delegitimizing doxing*

Digital citizenship merupakan sebuah norma perilaku terkait penggunaan teknologi. Warga digital adalah seseorang yang melalui pengembangan berbagai kompetensi secara aktif, positif, dan bertanggung jawab dalam komunitas *online* dan *offline*, baik lokal, nasional, maupun global. Karena teknologi digital bersifat *disruptif* dan terus berkembang, pengembangan kompetensi adalah proses seumur hidup yang harus dimulai sejak masa kanak-kanak di rumah dan di sekolah, di lingkungan pendidikan formal pendidikan formal, informal, dan non-formal.

1.1.2. Simpulan Khusus

Pada simpulan khusus ini, memaparkan hasil dari penelitian yang dilakukan, setelah dianalisis dan diolah lebih mendalam, maka peneliti memaparkan kesimpulan khusus yang dibuat dengan menyesuaikan rumusan masalah yang dibahas sehingga kesimpulan khusus yang dipaparkan adalah sebagai berikut :

1. *Doxing* atau penyebaran informasi pribadi tanpa izin merupakan salah satu bentuk kejahatan siber yang semakin marak terjadi di era

digital termasuk di kota Bandung. Kejahatan ini mencakup perilaku mengumpulkan, mempublikasikan, dan menyebarkan data pribadi seseorang untuk tujuan yang biasanya negatif. Beberapa temuan menunjukkan bahwa *doxing* dilakukan dengan niat kurang baik dan melibatkan riset mendalam terhadap subjek. *Doxing* merupakan tindakan dengan konotasi negatif hal ini karena melanggar privasi seseorang dengan tujuan baik untuk mempermalukan, mengintimidasi, atau merusak kredibilitas seseorang. Dalam konteks hukum di Indonesia, *doxing* sudah masuk ke dalam pelanggaran yang telah diatur didalam Undang-Undang Informasi dan Transaksi Elektronik serta Undang-Undang Perlindungan Data Pribadi. Keduanya mengatur larangan penggunaan, pengungkapan, dan distribusi data pribadi tanpa izin pemiliknya. *Doxing* dapat digolongkan menjadi tiga jenis: *deanonymizing*, *targeting*, dan *delegitimizing*. Di Bandung, kasus *doxing* sering kali tidak berdiri sendiri tetapi berkaitan dengan pelanggaran lain, seperti pinjaman online ilegal dan pencemaran nama baik. Hal ini menunjukkan bahwa *doxing* adalah kejahatan yang kompleks dan memerlukan penanganan yang serius dari berbagai pihak, termasuk penegak hukum, pemerintah, dan masyarakat, untuk melindungi data pribadi dan mencegah penyalahgunaannya.

2. Faktor-faktor yang menyebabkan *doxing* bisa dibagi menjadi dua: internal dan eksternal. Faktor internal yang bisa menyebabkan tindakan *doxing* ini yaitu kelalaian pengguna, kurangnya kesadaran tentang keamanan digital, dan ketidakpahaman tentang jejak digital. Adapun faktor eksternal sendiri meliputi adanya niat jahat dari orang lain, adanya kesempatan/ketersediaan informasi, adanya anonimitas, dan kurangnya regulasi dan penegakan hukum. *Doxing* adalah pintu awal dari kejahatan siber lain dan dapat menimbulkan kerugian baik material maupun imaterial bagi korban.
3. *Doxing* sebagai tindakan menyebarluaskan informasi pribadi tanpa izin, bertentangan dengan prinsip-prinsip *digital citizenship*.

Berdasarkan penjabaran Ribbel sendiri kewarganegaraan digital mencakup perilaku aman, bertanggung jawab, dan etis di dunia digital. Terdapat sembilan aspek utama yang membentuk kewarganegaraan digital, seperti etika, komunikasi, pendidikan, dan tanggung jawab. Hasil temuan menunjukkan bahwa masyarakat memahami *digital citizenship* sebagai norma dan nilai yang harus dijaga di dunia digital. Namun, tindakan *doxing* ini melanggar etika dan norma tersebut, serta prinsip-prinsip Pancasila. Berbagai pendapat masyarakat dan ahli menggarisbawahi bahwa *doxing* adalah tindakan yang tidak etis dan merugikan, tidak mencerminkan perilaku warga digital yang baik. Dalam perspektif *digital citizenship*, tindakan *doxing* jelas merupakan pelanggaran hukum dan etika. *Digital citizenship* mengajarkan penggunaan teknologi secara positif dan bertanggung jawab, sejalan dengan hukum positif di Indonesia yang melarang tindakan melanggar privasi seperti yang tercantum dalam Kitab Undang-Undang Hukum Pidana dan Undang-Undang Informasi dan Transaksi Elektronik serta Undang-Undang Perlindungan Data Pribadi. Secara keseluruhan, *digital citizenship* dan hukum diperlukan untuk membangun masyarakat yang aman dan bertanggung jawab di dunia digital. Kolaborasi dan edukasi dari berbagai pihak sangat penting untuk meningkatkan kesadaran dan pemahaman tentang pentingnya menjaga data pribadi dan mematuhi etika digital.

5.2. Implikasi

Penelitian yang berjudul "Analisis Kejahatan Siber *Doxing* dalam Perspektif *Digital citizenship* (Studi Kasus di Kota Bandung)" merupakan penelitian yang berfokus pada permasalahan kejahatan digital terkait publikasi identitas pribadi tanpa izin di media sosial. Penelitian ini merupakan suatu cara agar kita semua bisa melek terhadap pentingnya identitas kita sendiri di dunia digital. Identitas yang di publikasi di khalayak umum bisa jadi mengundang kejahatan lain kepada diri kita. Maka dari itu diperlukannya edukasi dan

penjelasan apa itu kejahatan *doxing* dan edukasi pentingnya identitas di dunia digital sekarang ini.

Dengan adanya penelitian ini, diharapkan dapat membuka pengetahuan kita semua terkait dampak adanya kejahatan di era baru sekarang ini khususnya yang berhubungan dengan identitas pribadi kita. Maka dari itu penting bagi para pemerintah, akademisi, dan para penggerak literasi digital untuk bisa mengedukasi masyarakat terkait dengan pentingnya identitas digital. Dari edukasi inilah kemudian masyarakat bisa mengetahui perbuatan penyebaran identitas pribadi seseorang itu dilarang dan bisa menimbulkan kerugian bagi orang lain. Barulah kemudian akan muncul kesadaran dalam memanfaatkan digitalisasi dengan baik di masyarakat yang mana hal tersebut mencerminkan *digital citizenship*.

5.3. Rekomendasi

Pada subab rekomendasi ini, peneliti memberikan beberapa rekomendasi berkaitan dengan penelitian yang berjudul "Analisis Kejahatan Siber *Doxing* dalam Perspektif *Digital citizenship* (Studi Kasus di Kota Bandung)" yang diharapkan menjadi pengingat ataupun perbaikan untuk kedepannya bagi setiap pihak serta bisa menjadi referensi kedepanya.

1. Jajaran Polri/Polda

Untuk meningkatkan efektivitas penanganan kasus *doxing*, jajaran Polri/Polda perlu memperkuat unit-unit khusus seperti *cybercrime*. Penguatan ini mencakup penambahan sumber daya manusia, teknologi, serta peningkatan keterampilan melalui pelatihan khusus. Petugas yang memahami secara mendalam modus kejahatan siber akan lebih siap dalam menangani kasus *doxing*. Selain itu, kerjasama yang erat dengan platform media sosial sangat penting dalam mendeteksi dan menindak pelaku kejahatan ini. Dengan dukungan teknologi dan kolaborasi yang baik, penegakan hukum terhadap kejahatan siber dapat dilakukan dengan lebih efektif.

2. Dinas Komunikasi dan Informatika (Diskominfo)

Diskominfo memiliki peran penting dalam meningkatkan kesadaran publik mengenai bahaya *doxing*. Kampanye kesadaran digital yang

mencakup edukasi tentang perlindungan data pribadi dan dampak negatif dari kejahatan siber perlu dijalankan secara intensif. Selain itu, Diskominfo harus terus meninjau dan memperbarui regulasi terkait perlindungan data pribadi, serta memastikan bahwa sanksi terhadap pelanggaran seperti *doxing* ditegakkan dengan tegas. Pengawasan terhadap konten digital juga harus diperkuat untuk mencegah tersebarnya informasi yang merugikan masyarakat.

3. **Jajaran Pemerintah Kota Bandung**

   Sebagai pemimpin di tingkat lokal, Pemerintah Kota Bandung dapat mempelopori inisiatif yang mendukung kewarganegaraan digital, khususnya dalam melawan kejahatan siber seperti *doxing*. Pemerintah kota dapat memfasilitasi program edukasi di sekolah dan komunitas yang berfokus pada penggunaan internet yang aman dan etis. Selain itu, penyediaan pusat layanan pengaduan bagi korban kejahatan siber merupakan langkah penting untuk memberikan dukungan dan perlindungan bagi warga yang terkena dampak.

4. **Akademisi**

   Akademisi memiliki tanggung jawab untuk melakukan penelitian lanjutan terkait dampak sosial dan psikologis dari *doxing*. Penelitian ini dapat memberikan wawasan lebih mendalam yang bermanfaat bagi pembuat kebijakan dan masyarakat umum. Selain itu, pendidikan tentang etika digital perlu diintegrasikan ke dalam kurikulum pendidikan tinggi, terutama di jurusan yang berhubungan dengan teknologi informasi dan komunikasi. Kolaborasi antara disiplin ilmu, seperti hukum, komunikasi, dan teknologi, juga diperlukan untuk memahami fenomena *doxing* secara komprehensif dan mencari solusi yang efektif.

5. **Masyarakat yang Menggunakan Media Sosial/Teknologi**

   Masyarakat pengguna media sosial harus lebih waspada terhadap risiko yang ada di dunia digital, termasuk ancaman *doxing*. Kesadaran akan pentingnya menjaga privasi dan berhati-hati dalam membagikan informasi pribadi harus terus ditingkatkan. Masyarakat juga perlu didorong untuk segera melaporkan tindakan *doxing* kepada pihak berwenang jika menjadi

korban atau mengetahui adanya kasus tersebut. Edukasi mandiri dan saling berbagi informasi mengenai keamanan digital merupakan langkah penting untuk menciptakan lingkungan *online* yang lebih aman.

6. **Orang Tua**

   Orang tua berperan penting dalam melindungi anak-anak dari ancaman *doxing* dan kejahatan siber lainnya. Pendampingan dalam penggunaan internet dan media sosial sangat diperlukan, termasuk mengajarkan anak-anak tentang pentingnya keamanan *online* dan menjaga privasi. Orang tua juga harus menciptakan lingkungan komunikasi yang terbuka, sehingga anak-anak merasa nyaman untuk melaporkan jika mereka mengalami atau melihat hal-hal yang tidak pantas di internet. Penggunaan fitur kontrol parental juga disarankan untuk membatasi akses anak-anak ke konten yang tidak sesuai.

7. **Pelajar, Remaja, dan Anak-anak**

   Pelajar, remaja, dan anak-anak perlu memahami bahwa menjaga privasi di dunia digital adalah hal yang sangat penting. Mereka harus belajar untuk lebih selektif dalam membagikan informasi pribadi di media sosial dan menyadari potensi bahaya yang dapat timbul dari perilaku tidak bertanggung jawab. Selain itu, mereka juga harus didorong untuk mengikuti program edukasi tentang *digital citizenship* dan keamanan *online*, yang akan membantu mereka menjadi pengguna internet yang lebih bijaksana dan bertanggung jawab.

8. **Program Studi Pendidikan Kewarganegaraan**

   Program studi Pendidikan Kewarganegaraan memiliki peran strategis dalam membekali mahasiswa dengan pemahaman tentang *digital citizenship* dan bahaya kejahatan siber seperti *doxing*. Materi tentang etika digital dan kewarganegaraan digital perlu diintegrasikan ke dalam kurikulum, sehingga lulusan memiliki kompetensi yang relevan dengan tantangan zaman. Pelatihan praktis bagi mahasiswa tentang penggunaan internet yang bertanggung jawab juga penting untuk mempersiapkan mereka dalam menghadapi dunia digital yang semakin kompleks. Selain itu, kolaborasi dengan ahli IT dalam pengembangan modul pendidikan yang *up-*

to-date akan memperkaya kurikulum dan memastikan relevansinya dengan perkembangan teknologi.